STORAGECRAFT®

ShadowProtect User Guide

StorageCraft Copyright Declaration

Table of Content

ShadowProtect User Guide

Welcome to the StorageCraft® *ShadowProtect® User Guide*. This edition covers ShadowProtect versions up to **v5.2.3** of these products:

- Desktop
- Server
- Small Business
- Virtual

and related sections for the ShadowProtect IT Edition and the StorageCraft Recovery Environment.

This Guide describes the ShadowProtect technology, how to use the product, and how to get the most out of ShadowProtect. While ShadowProtect comes in multiple editions, most of the differences between these editions relate to the associated user license. When there is specfic information for an edition, this Guide notes this.

Edition	Description
ShadowProtect Desktop	Provides volume backup and restore options for a single desktop system. This edition is most suitable for home use.
ShadowProtect Server	Provides backup and restore options for server operating systems. ShadowProtect Server requires a separate license for each installed OS.
ShadowProtect for Small Business	Provides backup and restore options for Microsoft Small Business Server (SBS). ShadowProtect SBS requires a separate license for each installed OS.
ShadowProtect MSP	Provides a subscription-based licensing model for Managed Service Providers (MSP) that want to provide disaster recovery solutions for their clients.
ShadowProtect Virtual	Provides a VM-based licensing model for disaster recovery in a virtualized environment.

This Guide includes the following major sections:

- ShadowProtect Overview
- How ShadowProtect Works
- Installing ShadowProtect
- Understanding ShadowProtect Console
- Create a Backup Image
- Mounting Backup Image Files
- Restoring a Volume
- Image Conversion Tool
- Using ISOTool
- Using ImageReady
- Remote Management
- Using VirtualBoot
- Other Operations
- Best Practices

Additional Information

- For emerging issues and other resources, see the following:
  - The New Features in this Version page.
  - The ShadowProtect ReadMe file available online.
  - The StorageCraft technical support Web site at www.storagecraft.com/support.html.
- This User Guide is also available in the ShadowProtect user interface from the Help menu.
- The StorageCraft Glossary of technical terms.

Documentation Conventions

⚠ This symbol designates **Note** or **Warning** text that highlights important information about the configuration and/or use of ShadowProtect.

1 ShadowProtect Overview

Review these topics as you prepare to install and use ShadowProtect:

- Features and Components
- Usage Scenarios

1.1 Features and Components

For a complete version history of product updates, refer to the online ShadowProtect ReadMe document.

Component	Features
ShadowProtect Console	This console manages the disaster recovery configuration on your Windows system. The console can: • Configure backup jobs that run unobtrusively in the background using Microsoft VSS (Volume Shadow Copy Service). • Store backups on any accessible media including network storage (SAN, NAS, iSCSI), removable drives (USB, FireWire), and optical media (CD, DVD, Blu-Ray). • Verify backup images to ensure data integrity. • Create compressed and encrypted backup image files for efficiency and security. • Run wizard-based recovery of files, folders, or a complete data volume, to an exact point in time. • View backup images for quick file and folder recovery. • Mount any backup image file as a virtual disk using VirtualBoot. • Remotely manage system backup and recovery operations.
ShadowProtect Backup Agent	The engine that creates a system's point-in-time backup images. The ShadowProtect console manages the operation of this backup agent.
StorageCraft Recovery Environment	A bootable environment for disaster recovery which doesn't require installing software. StorageCraft offers both a recovery environment based on Windows and the new Recovery Environment-CrossPlatform based on Linux which also restores all supported Windows systems. Either environment can: • Access all critical features of the ShadowProtect Console from a standalone disaster recovery environment. • Load from a bootable CD or USB drive. • Restore a system (bootable) volume quickly and easily. • Back up a non-bootable system before attempting a restore operation. • Use Hardware Independent Restore (HIR) to restore to different hardware, or to virtual environments (P2P, P2V, V2P). For more information about the Recovery Environment, see the StorageCraft Recovery Environment User Guide.

ImageManager

StorageCraft also offers ImageManager which provides policy-driven services for managing backup image files. These include:

- Consolidation of Incremental backup image files into daily, weekly, and monthly consolidated image files that greatly reduce the number of files in an image chain.
- Verification and re-verification of backup image files, including consolidated files.
- Replication of backup image files to a local drive, a network share, or an off-site location (using FTP, intelligentFTP, or ShadowStream).
- Head Start Restore (HSR) lets you restore a backup image while ShadowProtect continues to add incremental backup images to it. This lets you greatly reduce the downtime associated with hardware failure or hardware migration tasks.

For more information about ImageManager features, see the ImageManager User Guide.

1.2 ShadowProtect Usage Scenarios

ShadowProtect supports a variety of backup and recovery scenarios, depending on your needs. These include:

- ShadowProtect Console Scenarios
- VirtualBoot Scenarios

ShadowProtect Console Scenarios

Here are several common use cases for ShadowProtect:

Live Backup

Problem: I don't want to shutdown a system every time I want to create a system backup image.

ShadowProtect Solution: By leveraging disk imaging with existing Windows snapshot technology, ShadowProtect lets you create live system backups without any system downtime. ShadowProtect creates live backup images that include a system's operating system, critical data and configuration settings.

Create Full and Incremental Backup Images

Problem: Making a full backup image every time I backup a system is very time consuming. I need to be able to make incremental backup images to save time and space.

ShadowProtect Solution: ShadowProtect uses a sector-based backup strategy that lets it backup just the changes to a file in an Incremental backup image. Sector-based incremental backup is the quickest and most efficient way to take an incremental backup.

Once you have an initial full backup, you can create regular incremental backup images from that point forward to support an accurate restoration.

Individual Folder and File Restore

Problem: Restoring individual files and folders traditional backup systems, such as a tape drive, can be very difficult and time-consuming...assuming I can even find the necessary data in the first place. I need a quick and easy method to recover lost files or folders.

ShadowProtect Solution: Use the ShadowProtect Backup Explore Wizard to mount a backup image file as a volume using a Drive letter or mount point. Once mounted, you can explore and recover individual files and folders from the backup image. Disk-based backup images provide fast file access, and you can even share backup images so Since the backups are disk-based, theprocess is very fast and easy and uses Windows Explorer. The IT administrator can mount a backup image and share this with end users who can select the files and folders they need to restore.

Update an Existing Backup Image

Problem: I have an existing backup image, but need to update a driver in that image, or clean a virus or other malware from the backup image before restoring files. I don't want to have to clean the system, then re-create the backup image before using it to restore a system.

ShadowProtect Solution: Because you can mount ShadowProtect backup image files as read/write volumes, you can modify and repair backup images as needed. ShadowProtect saves these backup image changes as a separate Incremental image file.

VirtualBoot Scenarios

The following scenarios introduce several possible use cases for VirtualBoot:

Historical Data Access

Problem: After transitioning to a new financial management system, you are audited. To satisfy the audit, you need access to historical tax records stored in the proprietary format of the old financial software. Unfortunately, you no longer have the old software, so you cannot access your historical tax records.

VirtualBoot Solution: Rather than trying to restore a complete backup image that contains the old financial software, use VirtualBoot to boot the backup image, which gives you access to both the application and the data from your system at the time of the backup. By preserving the applications with the data, you can greatly extend the lifespan of your data.

Software Testing

Problem: You need to find out how some new software performs on your production system, but you don't want to risk having any problems.

VirtualBoot Solution: VirtualBoot the latest backup of your production system, then install the software in the virtual machine. You can evaluate the software performance using your system's actual production environment without any risk to your production system.

Backup Image Testing

Problem: You need to confirm that your backup images restore properly and that they provide access to all your mission critical applications and data.

VirtualBoot Solution: VirtualBoot a recent backup image and you can verify that the restored applications and data perform as expected..

Hardware Failure

Problem: You have a database server and the 20TB disk array crashes. You need to get the system back on-line and replace the disk subsystem.

VirtualBoot Solution: This solution is a three-step process:

1. VirtualBoot the latest backup image of your database server so users can continue using the database. The interim VM solution performs well because there is no file conversion required. StorageCraft provides native support for its backup image files in the VirtualBox environment.

As part of this process, configure ShadowProtect to continue creating Incremental backups in the VM, preferably every 15 minutes. These Incremental backups are part of the original backup image chain. ShadowProtect has VirtualBox store the VM-generated Incremental backups in native VDI files. While these files are relatively tolerant of VM host crashes, or VirtualBox.exe or VBoxSvc.exe process crashes, they might become corrupt and prevent the VM from restarting. If this happens, create a new VirtualBoot VM, using as the VM source the latest Incremental backup created in the prior VM.

Warning: To continue uninterrupted Incremental backups in a VirtualBoot VM, the ShadowProtect backup job that creates the backup image files must use a ShadowProtect Destination Object of type Network Share (see Destinations).

2. Start a HeadStart Restore (HSR) on the database server's new disk subsystem (For more information, see the ShadowProtect ImageManager User Guide).

3. Once the HSR catches up to the most current Incremental, created in the VM, take the VM offline and finalize the HSR installation on the new disk subsystem (a quick operation), then bring the database server hardware back on-line.

Note: Once the replacement VM is online and continuing the Incremental backup image chain, you can recover from a hardware failure in several different ways:

- Restore to the original hardware, once repaired.
- Restore to new hardware (using StorageCraft Recovery Environment's Hardware Independent Restore (HIR)).
- Restore permanently to a VM environment by using HSR to restore to a VHD or VMDK virtual machine hard disk file.

2 How ShadowProtect Works

A ShadowProtect backup image file is a point-in-time representation of a computer volume. It is not a standard file copy of the volume, but rather a sector-by-sector duplicate of the volume. In the event that you need to recover data, you can mount a backup image file (using the ShadowProtect Mount utility) and view its contents as if it were a regular volume. You can recover specific files and folders from the image or you may recover the entire volume to the exact point in time that the backup image was taken.

This section includes the following topics:

- Create a Backup Image
- Restore a Backup Image
- Backup Image Files

2.1 Create a Backup Image

A *backup image file* is a sector-by-sector representation of the volume at the time the volume snapshot was taken. ShadowProtect writes the backup image file to the designated storage media. Options include network storage (SAN, iSCSI, NAS, etc.), removable storage (USB / FireWire), and optical storage (CD, DVD, Blu-ray). The amount of time it takes to write the backup image file depends upon the system hardware and the size of the image file. For information about configuring and creating backup image files, see Creating Backup Image Files and Backup Image Files.

Creating a ShadowProtect backup image involves two components--the Snapshot driver and Microsoft's VSS. Using Microsoft VolSnap and VSS (available with Windows Server 2003, Windows XP, or later), the ShadowProtect driver creates a point-in-time snapshot of the volume to protect. The entire process of taking a snapshot takes only seconds and does not interfere with system operation.

ShadowProtect may use different combinations of VSS and snapshot driver depending on the operating system and application:

Snapshot	Supported OS	Image Speed	Quality	Comments
StorageCraft VSM with VSS	Windows XP / 2003 and later	Fast	Best	• Manages VSS-aware applications to achieve best quality backups. • Uses script files to manage applications that are not VSS-aware to improve backups • Can create incremental backup files
Microsoft VolSnap with VSS	Windows XP / 2003 and later	Slow	Best	• VSS-aware applications are managed automatically to achieve best backups. • Uses script files (before and after the snapshot) to manage non-VSS-aware applications and improve backups. • Cannot create incremental image files.
StorageCraft VSM direct	Windows 2000	Fast	Good	• Uses script files (before and after the snapshot) to manage applications and improve backups. ⚠ **Note:** Windows 2000 does not support VSS, so VSM Direct is the only option for this platform.

ShadowProtect also includes two features for working with backup images: the Backup Scheduler and the Image Conversion Tool.

The ShadowProtect Backup Scheduler

The ShadowProtect Backup Scheduler can:

- Configure automated backup jobs to protect volumes.
- Schedule thse full image or incremental images (as often as every 15 minutes).
- Manage the retention of backup image sets.

The Image Conversion Tool

The ShadowProtect Image Conversion tool simplifies image management of existing image files. The tool can:

- Consolidate files in an image set
- Modify password encryption
- Enable compression
- Merge or split image files

2.2 Restore a Backup Image

Once you create a backup image, you can use this image to restore data in two ways:

Recover individual files and folders

Use the ShadowProtect Mount utility to open an image file as a volume either as a drive letter or a mount point. The Mount utility can efficiently mount hundreds of backup images simultaneously if needed. These mounted files preserve the Windows volume properties of the original. Users can access the backup image file just as they would if the volume were on a hard disk. This includes modifying and saving changes to the temporary volume as an incremental backup file.

For more information see Mounting Backup Image Files.

Restore entire volumes

Use the ShadowProtect console's Restore Wizard to restore an entire data volume from a backup image file. Use the StorageCraft Recovery Environment to restore a system (boot) volume.

For more information see Restoring a Volume.

2.3 Backup Image Files

ShadowProtect uses the following types of backup image files:

Backup Images	Description
Full .spf	A stand-alone image file that represents a disk volume at a specific point-in-time. Full backup image files do not rely on any other files.
Incremental .spi	An image file that contains volume changes relative to another backup image file. You can create Incremental backup image files relative to Full backup images or other Incremental backup images. ShadowProtect also creates an Incremental image file when an existing image file is mounted as a read/write volume and modified. Incremental backup image files let ShadowProtect offer multiple volume backup strategies, including differential and incremental backup options. See Glossary for information about these backup strategies.
Spanned .sp_#_	Image files that belong to a spanned image set. Spanned image sets are made by breaking a backup image file into pieces for increased portability (for example, to save the image file on multiple CDs or DVDs). The actual spanned image file name replaces the pound sign (#) with a number that indicates the position of the file within the spanned image set.
ImageManager -cd.spi -cw.spi -cm.spi	Image files that have been automatically collapsed by ImageManager. The suffix before the file extension indicates if the file is a daily, weekly or monthly collapsed backup files.
.spk	A password key file used to encrypt backup image files.
.spwb	A temporary "write-back" file used to save changes for a mounted image file volume.
.cr	A rolling file used by ImageManager consolidation
.bitmap	A data file used in optimizing ImageManager consolidation

File Naming Conventions

The ShadowProtect naming convention identifies the file and its relationship to, and dependencies on, other backup image files. The syntax is:

```
<volume-identifier>-b_<base-seq>-d<diff-seq>-i<inc-seq>.<extension>_
```

volume-identifier: Identifies the volume that the backup image file represents.

base-seq: The base image file sequence number. This either identifies:

- the sequence number of this file or
- the base image file upon which this file is dependent.

diff-seq: The Differential backup sequence number. This either identifies:

- the sequence number of this file or
- the differential image file upon which this file is dependent.

inc-seq: The Incremental backup sequence number. This either identifies:

- the sequence number of this file or
- the incremental image file upon which this file is dependent.

extension: The file extension, which identifies if the file is a Full, Incremental, or Spanned backup image file.

File Type Extension	Description
`C_Vol-b001.spf`	**Full image** of the `C:` volume.
`C_Vol-b001-d001-i000.spi`* or `C_Vol-b001-d001.spi`	**Differential image** of the `C:` volume with a dependency on the full backup image file `C_Vol-b001.spf`
`C_Vol-b001-d000-i000.spi`* or `C_Vol-b001-i001.spi`	**Incremental image** of the `C:` volume with a dependency on the full backup image file `C_Vol-b001.spf`
`C_Vol-b001-d001-i001.spi`	**Incremental image** of the `C:` volume with a dependency on the differential backup image file `C_Vol-b001-d001.i000` which in turn has a dependency on `C_Vol-b001.spf`.

*Backup image file names that include the "-d000" or "-i000" segment identifier indicate that the backup image file does not rely on any other differential or incremental backup image file.

NETGEAR ReadyDATA File Naming

Backup files saved to a NETGEAR device have a different naming convention:

`Year/Month/Day/Hour/Minute/Second plus a UTC offset`

where the *Hour/Minute/Second* is the system's Local Time--not UTC time. Using this nomenclature allows users to select the appropriate point in time they want to either mount or restore.

File Dependencies

The name of a backup image file identifies the files on which it depends. However, it is not possible to determine if other backup image files later in the chain are dependent on this file. Because of this, it is very important to use the Image Conversion tool to review dependencies prior to moving, modifying, or deleting backup images.

Warning: All backup image files are part of a chain--short or long. Deleting a backup image file on which other files depend makes the dependent backup image files useless. You cannot browse or restore files from these dependent backup image files.

The same is true of a full image file which anchors the chain. Deleting a full image file from an active chain causes ShadowProtect to start a new chain at the next scheduled backup. All the existing files cannot open without the missing full image.

3 Installing ShadowProtect

Before installing ShadowProtect, review the Requirements and the License and Install Options.

Note: Windows XP and Server 2003 users must log in with Local Administrator rights to use the ShadowProtect interface.

Caution: If the Windows Telnet Service is installed and running on the system, please review a potential error condition in Best Practices to avoid the snapshot driver failing to install.

To Install ShadowProtect

1. If you have a *ShadowProtect CD*, insert the disc into the system's CD drive.
   Note: If the installation does not start automatically, browse the ShadowProtect CD and click `AUTORUN` from the root of the CD.
   If you have downloaded the *ShadowProtect installer*, click on the .EXE file to launch the program.
2. Follow the steps of the Setup Wizard to complete the install.
   Note: To register ShadowProtect, you must install the language that matches the license key you purchase.
3. On the *Installation Type* page, select which type you want:

Complete	This installs all the ShadowProtect components
Custom	This option allows you to select which components to install and where to install them. For example, use this option if you want to install only the console on a particular system.

4. If you chose the *Custom* install option, select the ShadowProtect components to install, then click **Next** on each component page.

Management Console	Installs the ShadowProtect management interface (UI), which lets you manage both ShadowProtect operations for this system and remote systems if desired. This is the default.
Backup Agent	Installs the ShadowProtect Backup agent, which lets you manage ShadowProtect operations on this system remotely. This is the default.
Snapshot Driver	Installs the ShadowProtect VSS driver. This is the default and is required for optimal performance and data protection. Only deselect it if the system only runs non-VSS compliant software, such as some versions of Intuit QuickBooks.
Mount Services	Installs the ShadowProtect mount driver which adds the ability to mount and dismount a backup image file using the right-click menu in Windows Explorer. This is the default.
ISOTool	Installs a basic ISO utility to create, mount, or burn a copy of an ISO image.
VirtualBoot	Installs Windows Explorer integration for VirtualBoot. VirtualBoot launches a virtual machine using the selected system volume backup file. This is the default.
ImageReady	Installs the ImageReady image testing utility. **Note:** The Adobe CreativeCloud Suite install fails if StorageCraft ImageReady is already installed on the system.
SPDiagnostic Tool	Installs a tool that gathers detailed information about a ShadowProtect installation for use in troubleshooting issues for StorageCraft Support. The default is to not install the tool.

   ⚠ **Note**: To mount a VHDX backup on a system with a custom install of ShadowProtect, be sure the install includes at least the ShadowProtect Backup Agent. (It does not have to include the SnapShot Driver.) Otherwise, the VHDX mount fails.

5. In the Installation Complete page, select **Yes, I want to restart my computer now**, then click **Finish**.
   If you cannot restart the computer immediately, select **No, I will restart my computer later**.
   Note: You must restart the computer before attempting to use ShadowProtect to create backups.
6. Remove the ShadowProtect CD (if used) from the system's CD drive.

Upgrading ShadowProtect

If this is an upgrade to an existing ShadowProtect installation, the wizard shortens this process.

Remote Install

To do a silent or push install of ShadowProtect:

1. Download and unpack the appropriate installation info file (the ISS) file for the version of ShadowProtect to install. Save this file to the same folder with the ShadowProtect setup program.
   Note: Although this ISS file shares the same extension as a Windows InstallShield file, it uses a different format and cannot be used by InstallShield.
2. Select ShadowProtect's *Management View* tab.
3. Click **Install** on the menu bar. The Push Install Wizard displays.
4. Follow the prompts to select the installer package (the Setup program for ShadowProtect). The Wizard populates the package details fields.
5. Click **Next**.
6. Provide the appropriate credentials to access the endpoint(s) for the push install.
7. Select the endpoint(s) that are destinations of the push install.
8. Optional: Provide the ShadowProtect product key to activate the endpoint(s) license(s).
9. Select *Reboot after install* as required to perform backups of the endpoint.
10. Specify a time to perform the reboot and a message to alert the endpoint user.
11. Click Next to review the push install configuration.
12. Click Next to begin the install.

ShadowProtect completes the install of the ShadowProtect agent on each of the selected endpoints.

3.1 Requirements

ShadowProtect has the following hardware and software requirements:

- Hardware Requirements
- Supported Operating Systems
- Supported File Systems
- Supported Storage Media
- MSP Requirements
- Multi-boot Environments

Hardware Requirements

Hardware	ShadowProtect
CPU	300 MHz or higher Pentium-compatible CPU
Memory	The greater of 256 MB or the Operating System minimum
Hard Drive space	50 MB free disk space
CD-ROM or DVD drive	Required only for CD installs or for Recovery Environment
Monitor	VGA or higher resolution
Clustering	ShadowProtect does not support Windows Cluster Shared Volumes (CSV)

Backup Destination Requirements

ShadowProtect can save backup files to external or network-attached drives. This third-party hardware may have its own requirements. (For example, the Netgear ReadyDATA system.) Please refer to the appropriate manufacturer for details.

Windows Clustering

ShadowProtect does not support Windows Cluster Shared Volumes (CSV). Windows Server 2012 failover cluster may use CSV, for example. Installing ShadowProtect on such a system may result in redirection of I/O related to clustered shared volumes.

Supported Operating Systems

Specific operating system support is dependent upon the edition of ShadowProtect that you purchase. ShadowProtect supports both 32-bit and 64-bit versions of many operating systems. Refer to the ShadowProtect ReadMe for the latest specific support details.

Edition	Description
ShadowProtect Desktop Edition	• Windows XP Family, including: ◦ XP Home ◦ XP Professional • Windows Vista Family, including: ◦ Vista Home Basic ◦ Vista Home Premium ◦ Vista Ultimate • Windows 7 • Windows 8 • Windows 8 Pro • Windows 8.1 x86 • Windows 8.1 x64 • Windows 8.1 Enterprise x86 • Windows 8.1 Enterprise x64 • Windows 2000 Workstation SP4 (Support for Hot Backup of the booted OS and Cold Backup from Recovery Environment.)
ShadowProtect Server Edition	• Window Server 2000 SP4 (Support for Hot Backup of the booted OS and Cold Backup from Recovery Environment.) • Windows Server 2003 family, including: ◦ Server 2003 Standard Edition ◦ Server 2003 Standard Edition R2 ◦ Server 2003 Advanced Edition ◦ Server 2003 Advanced Edition R2 ◦ Server 2003 Enterprise Edition ◦ Server 2003 Enterprise Edition R2 ◦ Server 2003 Datacenter Edition ◦ Server 2003 Datacenter Edition R2 ◦ Server 2003 Web Edition ◦ Small Business Server 2003 • Windows Server 2008 (including R2) 32-bit x86 and 64-bit x64 • Windows Server 2008 R2 Foundation • Windows Server 2008 • Windows Server 2012 family, including: ◦ Windows Server 2012 ◦ Windows Server 2012 Core ◦ Windows Server 2012 Foundation ◦ Windows Server 2012 Essentials ◦ Windows Server 2012 Standard ◦ Windows Sever 2012 Datacenter Hyper-V ◦ Windows Server 2012 R2 x64 Essentials ◦ Windows Server 2012 R2 x64 Foundation ◦ Windows Server 2012 R2 x64 Storage Server ◦ Windows Server 2012 R2 x64 Data Center ◦ Windows Hyper-V Server 2012 R2
ShadowProtect SBS Edition (Small Business)	• Small Business Server 2003 • Small Business Server 2003 R2 • Small Business Server 2008 • Small Business Server 2011 • Windows Server 2012 Foundation • Windows Server 2012 Essentials • Windows Server 2012 R2 Foundation • Windows Server 2012 R2 Essentials **NOTE:** ShadowProtect SBS does not activate on Windows Storage Server 2008 R2 Essentials or any version of standard version of Windows Storage Server or DataCenter. Using VirtualBoot with SBS requires substantial memory (up to 16GB) for full functionality.

ShadowProtect Virtual	ShadowProtect Virtual supports Windows guests in these hypervisors: • VMware • Microsoft Hyper-V • Red Hat KVM • Red Hat Enterprise Virtualization (RHEV) • Xen **NOTE:** ShadowProtect does not support • Windows Storage Spaces storage pools • Windows Server Cluster Shared Volumes

Note: Windows 2000 does not support either the ISOTool or the ImageReady utilities in ShadowProtect.

Supported File Systems

ShadowProtect supports the following file systems:

- FAT16
- FAT16X
- FAT32
- FAT32X
- NTFS
- MBR Disks
- GPT Disks
- Basic and Dynamic Volumes and Disks
- 4K/AF drives with 4096 byte sectors

ShadowProtect does not support:

- exFAT or ReFS file systems
- Windows Storage Spaces storage pools
- Windows Server Cluster Shared Volumes
- Using VirtualBoot with UEFI-based system volumes

ShadowProtect also does NOT backup any links created with the SUBST command (or calls to DefineDosDevice()) because such links reside *outside* of any persistent file system.

Restores

ShadowProtect performs restores from:

- SPF
- SPI

image files for data volumes.

Note: ShadowProtect does not support restores from VHD or VHDX files.

ShadowProtect and Microsoft Windows Deduplication

ShadowProtect includes support for Windows Deduplication (dedup) in several scenarios:

- Creating a backup of a dedup-enabled volume
- Using a dedup-enabled volume as a destination for backup images (note that this yields only a modest savings in space as ShadowProtect already compresses these image files)
- Mounting a backup file containing a dedup-enabled volume (the mounting system must have the Windows Dedup feature enabled)
- Using VirtualBoot a system volume backup that includes a data volume hosted on a dedup-enabled system.
- Restoring a backup file created from a dedup-eabled volume (the destination needs to have the Windows Dedup feature enabled to view all files)
- Restoring a backup file hosted on a dedup-enabled volume using ShadowProtect on the same machine as the dedup-enabled volume

However, ShadowProtect does not support:

- Mounting a backup file that is deduped or dependent on another backup file that is deduped.
- Restoring a backup file hosted on a dedup-enabled volume using Recovery Environment if any of the backup files have been deduped.

Supported Storage Media

ShadowProtect supports these storage media:

- Locally-connected hard drives or SSDs
- Removeable hard drives (USB or FireWire)
- Virtual drives (LUN) hosted on a local RAID controller
- Network drives (SAN, NAS, iSCSI)
- Optical media (CD, DVD, Blu-Ray)

ShadowProtect does not support:

- Windows Storage Spaces storage pools
- Windows Server Cluster Shared Volumes (CSV)

Note: Installing ShadowProtect on a system using CSV may result in redirection of I/O related to clustered shared volumes. This may preclude access to volumes.

The ShadowProtect Recovery Environment for Windows also supports restoring volumes from virtual disks in the Microsoft VHDx format (used by the NETGEAR ReadyDATA device for storing ShadowProtect backup images).

The Image Conversion feature of ShadowProtect supports these virtual disks:

- VMware VMDK
- Microsoft VHD
- Microsoft VHDX

Note: Hyper-V cannot attach and boot from a VHDX file converted from a system volume backup image. It can, however, mount and access the file.

Supported Sector Sizes

Contemporary hard drives and SSDs ship with a 4096-byte *physical* sector size. Most also support the 512-byte *logical* sector size. (These drives are often labeled 512e for "512 Byte Sector Size Emulation".) ShadowProtect supports backing up both 4096- and 512-byte logical sector sizes.

In the unusual situation of restoring a partition/volume from one logical sector size to another:

- 512 bytes per logical sector -> 4096 bytes per logical sector (and the destination does not support 512e)
- 4096 bytes per logical sector -> 512 bytes per logical sector

ShadowProtect will issue an error message during the restore if it encounters a mis-matched sector size.

MSP Requirements

The MSP version of ShadowProtect requires a 32-bit proxy configuration to access the Internet. Otherwise, ShadowProtect cannot activate its license. This is an issue as Windows 64-bit OSes configure only 64-bit proxy settings by default. Confirm that the proxy is configured for 32-bit (and not just 64-bit) applications. Once the Windows proxy supports both 32- and 64-bit applications, confirm the communication between the client and the proxy.

In particular, review the two MSP read-only fields in the ShadowProtect console under **Options** > **Agent Options** > **Agent NT Service Options**:

- Proxy Server
- Proxy Port

These settings should be the same as the Windows configuration in **Control Panel** > **Internet Options** > **Connections** > **LAN Settings** > **Proxy Server**. Use the Windows procedures to modify these settings as required.

For more information, see the StorageCraft MSP Portal Users Guide.

Multi-Boot Environments

If your system has multiple boot partitions, install ShadowProtect on each of the bootable Windows partitions. These installs guarantee that ShadowProtect recognizes changes to ShadowProtect-managed volumes from these secondary Windows environments. You do not need to activate ShadowProtect, but the snapshot driver (stcvsm.sys) must be available in each Windows partition.

This snapshot driver manages the fast incremental tracking in ShadowProtect. If you boot to an alternate OS environment where the snapshot driver is not loaded, ShadowProtect cannot track volume updates from that OS boot session. This means that your next Incremental backup misses any changes made from the alternate OS.

If one or more non-Windows operating systems, such as Linux, can write to a ShadowProtect-managed volume, make sure ShadowProtect recognizes those changes by creating a script. This script should execute during the startup/logon phase of the non-Windows OS. It should delete all VSM000.IDX (case-sensitive) files from the root directory of each ShadowProtect-managed volume. Removing these files forces ShadowProtect's stcvsm.sys to do a full differential/comparison backup when your primary Windows volume boots. This differential image file captures any changes made to the volume from the non-Windows OS.

3.2 License and Install Options

StorageCraft provides the following ShadowProtect license options:

License Type	Description
Purchased License	StorageCraft licenses ShadowProtect on a per-system basis (based on the number of systems for which you are making backups. For example, using ShadowProtect to backup 100 computers requires 100 licenses. Before using the software, review the complete End User License Agreement.
Evaluation License	StorageCraft provides an Evaluation version of the ShadowProtect software as a CD or ISO image file. Use this version to create and restore backup image files of system and data volumes as well as restore specific files and folders. (The Evaluation version includes the StorageCraft Recovery Environment to restore system volumes.) The Evaluation version expires and ceases to operate after the Evaluation period ends. Images created during the Evaluation period are fully compatible with the registered (purchased) version of the software.
Trial License	StorageCraft provides a Trial version of the ShadowProtect software as a free download. Use this version to create backup image files of system and data volumes as well as restore specific files and folders or data volumes. However, you cannot restore system volumes because the Trial version does not include the StorageCraft Recovery Environment. The Trial version expires and ceases to operate when the trial period ends. Images created during the trial period, however, are fully compatible with the registered (purchased) version of ShadowProtect.

NOTE: ShadowProtect licenses are language-specfic. Be sure to select this license language when installing ShadowProtect. Note that the ShadowProtect language does not have to match either the OS language or any related Language Packs or MUIs. (For example, a user could activate a German language install of ShadowProtect on an English language Windows system.)

ShadowProtect Virtual

ShadowProtect Virtual is a licensing model specifically designed for virtual environments. It allows you to purchase a single ShadowProtect Virtual license or licenses in 3, 6, 12, 24, or 50 license bundles..

ShadowProtect Virtual offers the same features and functionality available in ShadowProtect at a price point more appropriate to a virtualized environment.

⚠ **Note:** ShadowProtect Virtual licenses allow you to migrate or restore to a physical environment. However, once restored to a physical system, the virtual license does not permit ShadowProtect to continue making backups. You must use a standard ShadowProtect license to make backups in a physical environment.

ShadowProtect for Managed Service Providers

ShadowProtect for Managed Services Providers (SPMSP) is a subscription-based licensing option for Managed Service Providers (MSP) that want to provide disaster recovery services to their clients. ShadowProtect for Managed Services:

- Supports all types of Windows installations (Desktop, Server, SBS, etc.) using a single product installer.
- SPMSP licenses "call home" to StorageCraft servers on a daily basis to confirm that these licenses are still active. Because of this, SPMSP installs require Internet connectivity.
- An SPMSP license activation is valid for 30 days. As part of the "call home" process, SPMSP licenses auto-renew every 30 days unless:
  - The MSP or StorageCraft explicitly deactivates the license.
  - The license stops calling home, in which case it automatically deactivates

  The StorageCraft MSP Licensing Console (http://msp.storagecraft.com) lets MSPs create and manage SPMSP licenses, including remote license deactivation when needed.

3.3 Starting ShadowProtect

You can access ShadowProtect in two ways:

From Windows: Select **Start** > **All Programs** > **StorageCraft** > **ShadowProtect.**

From Recovery Environment: Make sure your system boot sequence is set to boot from the CD-ROM drive. Put the ShadowProtect CD in the system's CD-ROM drive, then boot the system. For more information about loading and using Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

Note: If ShadowProtect installs after ImageManager v6.5 or newer on the same system, the ImageManager Startup menu icons may not appear.

3.4 Activating ShadowProtect

When you purchase ShadowProtect, StorageCraft provides you with both a product serial number and an Evaluation version of the purchased product. We recommend you activate the product upon installation using the product serial number.

The Evaluation version provides you with 30 days of product access. During this time you must activate the product with the product serial number. If you do not activate the product within 30 days of installation, the product times out and stops functioning. (You can still activate the product after the end of the 30 days. However, any backup jobs you created will not run again until after you activate the product.)

NOTE: ShadowProtect licenses are language-specfic. Be sure to select this license language when installing ShadowProtect. Note that the ShadowProtect language does not have to match either the OS language or any related Language Packs or MUIs. (For example, a user could activate a German language install of ShadowProtect on an English language Windows system.)

You can activate ShadowProtect in two ways:

- Automatic Activation
- Manual Activation

⚠ **Note:** You can also deactivate a previously activated ShadowProtect installation. Deactivation frees up the product license for use on another system (see Deactivating ShadowProtect for more information).

OS Upgrades

You need to deactivate the ShadowProtect license and uninstall the software prior to upgrading an existing Windows 7 system to Windows 8 or a Windows 8 to Windows Pro. After the OS upgrade, reinstall ShadowProtect and reactivate the license. While the system preserves backup job configurations and other ShadowProtect settings, a best practice is to always create a new backup job for the upgraded system rather than continue an older, existing chain.

ShadowProtect Upgrades

If you upgrade ShadowProtect from one major revision to another, such as upgrading from v4.x to 5.x, you must have a valid and current maintenance agreement to continue to use the product (beyond a 30-day trial period). (Your existing license works for minor revision upgrades, such as from v4.1.5 to 4.2.0.)

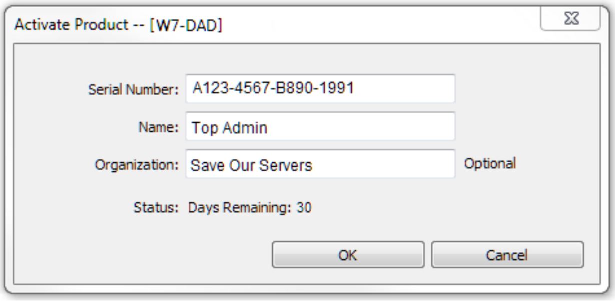
If you have a current maintenance agreement, to upgrade your ShadowProtect license:

1. Perform the upgrade.
2. After the upgrade, ShadowProtect displays *30-day Trial* under License in the navigation panel. Select **Help**>**Product Activation**.ShadowProtect displays the existing serial number (which has the maintenance agreement) along with the Name and Organization fields.
3. Enter a Name and/or organization.
4. Click **Activate** to re-activate this existing license for use with the new version of ShadowProtect.
5. Restart ShadowProtect if requested.

ShadowProtect displays *Active* under License in the navigation panel.

Automatic Activation

StorageCraft provides automatic activation for ShadowProtect installations.



Activate Product -- [W7-DAD]

Serial Number: A123-4567-B890-1991

Name: Top Admin

Organization: Save Our Servers Optional

Status: Days Remaining: 30

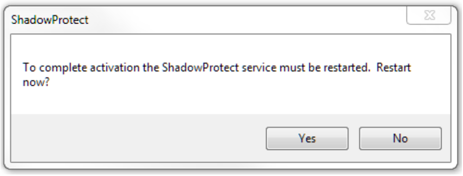
Note: There is a manual activation option If the system does not have Internet access. This option is on the StorageCraft website.

To activate ShadowProtect automatically

1. Start ShadowProtect.
   For more information, see Starting ShadowProtect.
2. From the Menu Bar select **Help** > **Product Activation**.
3. In the Product Activation dialog box, provide the requested information, then click **OK**.

   Product Serial Number Enter the serial number that you received when purchasing ShadowProtect.

   Name and Organization (Optional) Specify the name of the product user, purchaser, or organization.
4. If the activation is successful, click **Close**.
5. If the activation was not successful, review the message to determine why the activation was unsuccessful. To correct the problem, do one of the following:
   a) Review the information in the Product Activation dialog box for accuracy. Correct any errors, then **OK** to resubmit the activation request.
   b) If your computer cannot successfully communicate to the activation server or the Internet, wait for a while and try the activation process again..
   c) Ttry using the manual activation option to activate the software.
   c) Activation may fail if the software detects there are no more allowed activations for the serial number. Purchase additional licenses to increase the number of available activations. If you feel you received this message in error, contact StorageCraft Support .
6. ShadowProtect asks to restart the service:



ShadowProtect

To complete activation the ShadowProtect service must be restarted. Restart now?

Click **Yes** to restart the software. ShadowProtect is now activated.

Manual Restart

Clicking **No** in the Restart Now dialog delays activation until after a restart. (It also results in the ShadowProtect *Activate Product* dialog showing no serial number or other information.)

⚠ **Note:** Closing and reopening the ShadowProtect UI does not complete the activation or refresh the serial number in the Activate

Product dialog.

To restart the software after clicking No:

1. Close the ShadowProtect UI (if open).
2. Run Windows Services.msc.
3. Right-click **ShadowProtect Service**.
4. Select *Restart*. The ShadowProtect Service restarts.
5. Run ShadowProtect.
6. Select **Help** > **Product Activation**.

The activated serial number now displays along with the other information.

Activation during the Trial Period

You can install and run ShadowProtect without activating it for a period of 30 days. Once you choose to activate it, follow the steps listed.

Manual Activation

If you are unable to use the automated activation method, StorageCraft provides a manual activation option. This requires you to request an activation key online and manually apply it to your ShadowProtect installation.

Note: MSP installs do not support manual activation.

To get an activation key

1. Open a Web browser to http://www.storagecraft.com/activation.
2. Using the online form, provide:
   - Your ShadowProtect version.
   - Your customer name.
   - A valid email address to deliver the key.
   - The contents of the *license.id* file found in one of the two listed directories.
3. Click **Submit**.
4. Copy the activate.zip file from the response email or web form to the same directory containing the *license.id* file.
5. Unzip and run the activate.bat file.
   Note: This file is specfic to this system and its license.id file. It cannot be used to activate any other ShadowProtect install.
6. Start ShadowProtect.
7. Confirm that *Active* appears in the License field in the navigation panel.

You have successfully licensed ShadowProtect.

Deactivating ShadowProtect

ShadowProtect supports deactivation when:

- Upgrading a system from one version of Windows to another (for example, from Windows 7 to Windows 8),
- Upgrading from some older versions of ShadowProtect to another (see the ShadowProtect ReadMe for details).
- Retiring a system to make the license available for use on another system.

To deactivate a ShadowProtect license

1. Start ShadowProtect.
2. Select **Help** > **Product Activation**.
3. Click **Deactivate**.
   ShadowProtect displays a message stating you can no longer use this product key on this machine
4. Click **OK**.
5. Close ShadowProtect.

3.5 Uninstalling ShadowProtect

Use the standard Windows application removal tool to uninstall ShadowProtect.

To uninstall ShadowProtect

1. In Windows, select **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.
2. Double-click on *StorageCraft ShadowProtect*.
3. Select **Uninstall**.
4. Click **Next**.
   Note: The Uninstall program displays a warning if you have not deactivated the ShadowProtect license. If you proceed with the uninstall, you will have to reinstall the software later on to deactivate the license.
5. Click **OK** to acknowledge you have deactivated the ShadowProtect license.
6. Click **Next** to begin the uninstall.
7. Reboot the computer to complete the uninstall.

3.6 Upgrading ShadowProtect

Note: All ShadowProtect backup image files remain compatible with newer versions of ShadowProtect.

ShadowProtect upgrades come in three varieties:

Upgrades between minor revisions

Upgrades between minor revisions of ShadowProtect (such as between a 5.0 and 5.0.1 versions) simply require installing the new software. ShadowProtect retains all configuration settings.

To perform a minor revision upgrade:

1. On the *License Agreement* page, select **I accept the terms of the license agreement**, then click **Next**.
   Note: You must accept the license agreement to install ShadowProtect. (Click **Print** to print out the License Agreement if needed.)
2. On the *Ready to Install* page, click **Install**.The program completes the installation of ShadowProtect.
3. Click **OK** on the Reboot reminder page.
4. In the *Installation Complete* page, select **Yes, I want to restart my computer now**, then click **Finish**.
5. If you cannot restart the computer immediately, select **No, I will restart my computer later**. However, you must restart the computer before attempting to use ShadowProtect.
6. Remove the ShadowProtect CD (if used) from the system's CD drive.

Upgrades between major revisions

Upgrades between major revisions of ShadowProtect (such as from a 4.x to a 5.x versions) requires:

- Installing the new software
- Re-activating the new install (this requires a valid and current maintenance agreement.).

As with a minor revision upgrade, ShadowProtect retains all configuration settings for existing backup jobs.

To perform a major revision upgrade:

1. Perform a ShadowProtect upgrade using the minor revision steps.
2. After the upgrade, run ShadowProtect. The License field in the navigation pane shows "30-day Trial".
3. Select **Help** > **Product Activation**.ShadowProtect displays the previous activation key.
4. Fill in any remaining fields.
5. Click **OK** to re-activate.

ShadowProtect changes the license status to *Active*.

Upgrades to the Operating System

An upgrade to the operating system, such as:

- Windows 7 to Windows 8
- Windows 8 to Windows 8 Pro

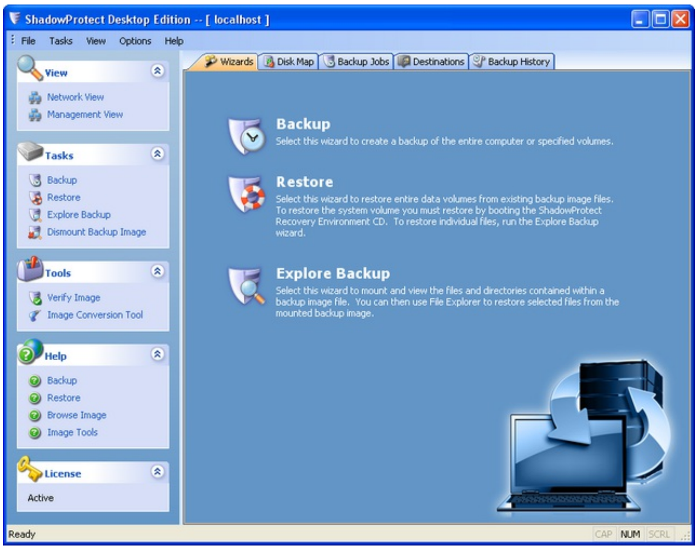
requires a reinstall and reactivation of ShadowProtect.

Note: With the many changes that occur with an OS upgrade, we recommend starting a new backup image chain to ensure an accurate OS restore should it be required later on.

Follow the steps in Deactivating ShadowProtect, Uninstalling ShadowProtect, and Installing ShadowProtect to complete the OS upgrade.

4 Understanding ShadowProtect Console

ShadowProtect Console includes most of the configuration and operation controls for ShadowProtect:



Backup
Select this wizard to create a backup of the entire computer or specified volumes.

Restore
Select this wizard to restore entire data volumes from existing backup image files. To restore the system volume you must restore by booting the ShadowProtect Recovery Environment CD. To restore individual files, run the Explore Backup wizard.

Explore Backup
Select this wizard to mount and view the files and directories contained within a backup image file. You can then use File Explorer to restore selected files from the mounted backup image.

The console is divided into four sections:

Menu Bar: Located at the top of the console, the Menu Bar provides access to general menus used to configure and operate ShadowProtect.

Navigation Panel: Located on the left side of the console, the Navigation Panel provides access to the tasks and tools used to configure and operate ShadowProtect.

Main Panel: Located in the center of the console, the Main panel uses Tabs to view ShadowProtect tasks and information.

Network Panel: Located on the right side of the console, the Network panel, or Network View, provides access to the Remote Management features in ShadowProtect.

4.1 Menu Bar

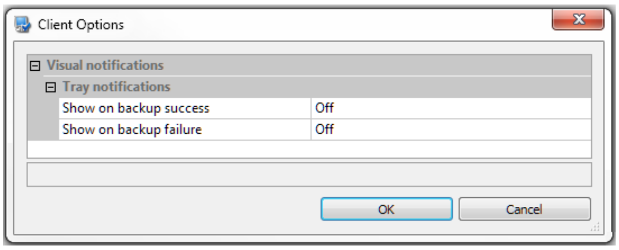
The ShadowProtect Console menu bar includes:

Menu	Description	Options
File	Accesses application-level options.	**Exit:** Closes the ShadowProtect UI.
Tasks	Accesses the ShadowProtect Wizards.	**Backup:** Launches the Backup Wizard (see Create a Backup Image). **Restore:** Launches the Restore Wizard (see Restoring a Volume). **Explore Backup:** Launches the Explore Backup Image Wizard (see Mounting Backup Image Files). **Dismount Backup Image:** Launches the Backup Image Dismount Wizard (see Dismounting Backup Image Files). **Verify Image:** Launches the Verify Image Wizard (see Verifying Backup Image Files). **Image Conversion Tool:** Launches the Image Conversion Tool Wizard**.** **Add Destination:** Opens the Destinations dialog box where you can create named destinations for backup image files. **Refresh Volumes Info:** Refreshes the ShadowProtect volume list for the current system.
View	Manages toolbar visibility.	**Status Bar:** Toggles a status bar at the bottom of ShadowProtect console to provide application and environment status information. **Task Panel:** Toggles visibility of the Navigation Panel.

Options	Accesses the ShadowProtect Agent options.	**Client Options:** Opens the Client Options dialog box where you can configure visual notifications for backup job success or failure. **Agent Options:** Opens the Agent Options dialog box, This box displays ShadowProtect agent configuration information and email notification settings for the current system. You can choose to send email notifications for either or both failed and successful backup jobs.
Help	Accesses the ShadowProtect help resources.	**Contents:** Opens a browser window to the online documentation. Use the Search box at the upper-right to locate specfic topics. **Note:** Help is only available when running ShadowProtect console, not the Recovery Environment. **Product Activation:** Opens the *Activation* dialog box, where you can activate (or deactivate) the ShadowProtect installation (see Activating ShadowProtect). **Check for Latest Version:** Queries for updates to the current ShadowProtect installation. If it finds an available update, it displays the URL to get the update. **Register:** Opens a browser to the Manual Activation page and request a product activation key (see Manual Activation). **About:** Displays the ShadowProtect version and copyright information. Click **System Info** in the About dialog to open the Microsoft System Information dialog box. This box contains detailed information about the computer.

Client Options

The ShadowProtect Client Options activates a visual notification of the system's backup success or failure:



Client Options

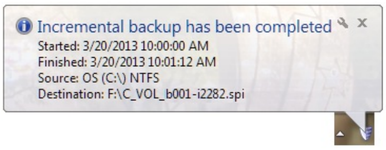
⊟ Visual notifications

⊟ Tray notifications

Show on backup success	Off
Show on backup failure	Off

The notifications default is Off. Use the dropdown menu to select On, then click **OK** to activate an alert.

At the next scheduled backup, ShadowProtect displays the notification:

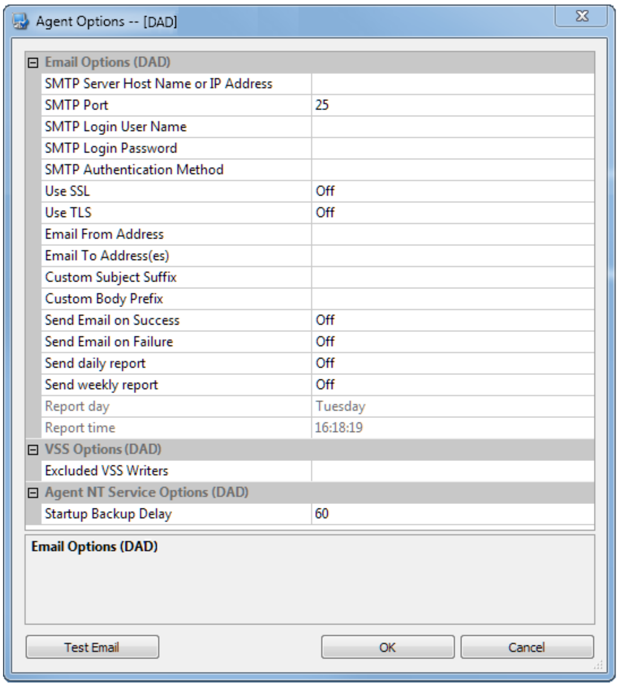


Incremental backup has been completed

Started: 3/20/2013 10:00:00 AM
Finished: 3/20/2013 10:01:12 AM
Source: OS (C:\) NTFS
Destination: F:\C_VOL_b001-i2282.spi

Agent Options

The Agent Options dialog configures this client's ShadowProtect email notifications. The dialog also displays configuration details.



Email Options (DAD)	
SMTP Server Host Name or IP Address	
SMTP Port	25
SMTP Login User Name	
SMTP Login Password	
SMTP Authentication Method	
Use SSL	Off
Use TLS	Off
Email From Address	
Email To Address(es)	
Custom Subject Suffix	
Custom Body Prefix	
Send Email on Success	Off
Send Email on Failure	Off
Send daily report	Off
Send weekly report	Off
Report day	Tuesday
Report time	16:18:19
VSS Options (DAD)	
Excluded VSS Writers	
Agent NT Service Options (DAD)	
Startup Backup Delay	60

Email Options (DAD)

Configure Email Notifications

1. Enter the requested SMTP server credentials and name.
2. Enter the To: and From: addresses. Include the administrator's address in the To: field to have ShadowProtect send copies to that address.
3. Select one or more types of email alerts: on Success, on Failure, Daily or Weekly reports.
   Note: Leaving all selections at their default value of "Off" tells ShadowProtect to send no alerts.
4. Click OK to save the configuration.
5. Click **Test Email** to confirm the configuration.

Configure VSS Options

ShadowProtect uses VSS to quiesce applications before taking a snapshot. Some VSS writers do not interact well with ShadowProtect and may causes issues such as a lengthy delay before ShadowProtect takes the snapshot. As a troubleshooting tool, ShadowProtect can exclude one or more VSS writers to identify which one is misbehaving.

To troubleshoot VSS writers:

1. Open a command prompt on the affected system.
2. Run `vssadmin list writers` to identify all installed VSS writers.
3. In the ShadowProtect console, select **Options** > **Agent Options** > **VSS Options** > **Excluded VSS Writers**.
4. Copy the VSS writer names into the field. Separate them using a semicolon (;).
5. Click **OK.**
6. Run a backup. Verify if the backup performs as expected. If so, the issue is with one of the VSS writers.
7. Remove a name from the list of excluded writers and rerun the backup until the problem returns. Retain this name in the excluded list.

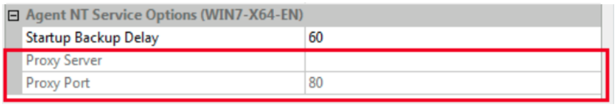
Configure NT Service Options

This section offers options for diagnostic or troubleshooting purposes:

Option	Default	Description
Startup Backup Delay	60 seconds	Sets the time to wait after the ShadowProtect service starts and before running a backup. For example, this setting allows time for the system to complete rebooting after the service starts.
Profile sbrun performance	Off	Set this option to ON at the request of StorageCraft Support to troubleshoot slow backup speeds. The statistics gathered appear near the end of the Backup Log.

ShadowProtect MSP Version

For installs using the ShadowProtect MSP version, the Agent Options dialog includes two additional non-editable items under the Agent NT Service Options:



⊟ Agent NT Service Options (WIN7-X64-EN)	
Startup Backup Delay	60
Proxy Server	
Proxy Port	80

These fields populate only when the system uses a proxy server. These options include:

Proxy Server	Identifies the client's proxy server as reported by Windows. Edit these proxy configuration details in **Control Panel** > **Internet Options** > **Connections** > **LAN settings** in the *Proxy Server* section.
Proxy Port	Identifies which port the client uses to communicate with the proxy server. The default is Port 80.

(See the MSP Portal guide for more details.)

4.2 Navigation Panel

The left-side Navigation panel provides quick access to ShadowProtect tasks and tools. Toggle the Navigation panel on or off by selecting **View** > **Task Panel**. The Navigation panel is organized into the following categories. You can collapse and expand each category, as desired.

Category	Description	Options
View	Displays or hides the Network View.	**Network View:** Toggles to display the list of nodes running the ShadowProtect Backup Agent (see Remote Management).
Tasks	Accesses ShadowProtect Wizards.	**Backup:** Launches the Backup Wizard. **Restore:** Launches the Restore Wizard. **Explore Backup:** Launches the Explore Backup Images Wizard. **Dismount Backup Image:** Launches the Backup Image Dismount Wizard.
Tools	Accesses ShadowProtect tools.	⚠ Note: Several tools are available only in the Recovery Environment. **Verify Image:** Launches the Verify Image Wizard. **Image Conversion Tool:** Launches the Image Conversion Tool Wizard. **Network Configuration:** (RE only) Launches the Network Configuration utility, where you can configure a computer's network access settings. **HIR Configuration:** (RE only) Launches the Hardware Independent Restore (HIR) utility, where you can restore a backup image to a different environment from which it was created. **Load Drivers:** (RE only) Opens the Load Drivers dialog box, where you can configure storage drivers for use in the Recovery Environment. **File Browser:** (RE only) A simple file browser that lets you browse files and folders of a backup image file. **Text Editor:** (RE only) A simple text editor. **Vista BCD:** (RE only) Launches the Vista BCD editor, where you can edit Boot Configuration Data (BCD) on systems running Windows Vista. **Partition Table Editor:** (RE only) A simple partition table editor. **UltraVNC:** (RE only) Launches the Remote Management utility, where you can configure remote access to systems running the Recovery Environment. **Select Your Time Zone:** (RE only) Launches the Time Zone utility, where you can adjust the system's time zone information. **Enable Logging:** (RE only) Opens the Logging dialog box, where you can configure ShadowProtect event logging.

Help	(Desktop/Server only) Accesses the online user guide. (Requires internet access.)	Opens a browser window to select the preferred language for the user guide. Select a language and the ShadowProtect User Guide. **Note**: Use the Search box at the upper-right of the page to locate specific topics.
License	(Desktop/Server only) Displays current licensing information for this ShadowProtect installation.	**Trial or Evaluation version:** Displays the number of days before the ShadowProtect installation expires. **Licensed version:** Displays "Active", meaning that the product is fully licensed and activated.
Info	(RE only) Display system information.	A quick reference to basic system information, including Computer Name, IP Address and Time Zone information.
Status	(RE only) Displays the current state of the system, including:	**Queued Tasks**: The number of queued tasks waiting to run. **Running Tasks**: The number of tasks currently running.

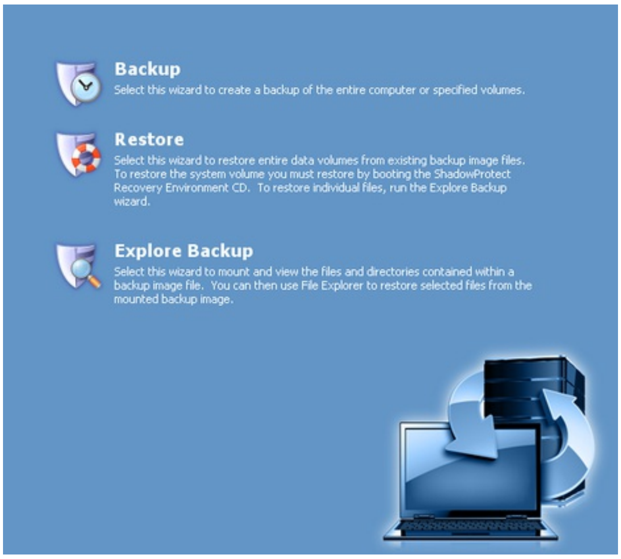
4.3 Tabs

The ShadowProtect Console provides the following pages in the Center panel:

- Wizards Tab
- Management View Tab
- Disk Map Tab
- Backup Jobs Tab
- Destinations Tab
- Backup History Tab

Wizards Tab

The Wizards tab is the default page in the Main panel. It provides access to three Wizards that guide users through the most common ShadowProtect tasks.



Backup
Select this wizard to create a backup of the entire computer or specified volumes.

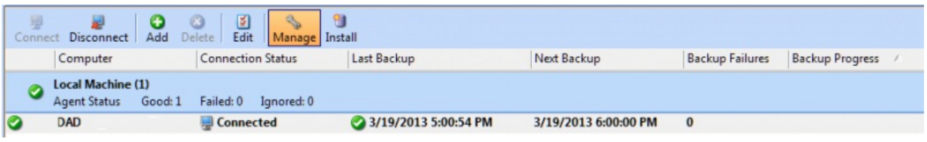
Restore
Select this wizard to restore entire data volumes from existing backup image files. To restore the system volume you must restore by booting the ShadowProtect Recovery Environment CD. To restore individual files, run the Explore Backup wizard.

Explore Backup
Select this wizard to mount and view the files and directories contained within a backup image file. You can then use File Explorer to restore selected files from the mounted backup image.

- **Backup:** Starts the Backup Wizard. This guides you through the creation of a backup job. For more information, see Create a Backup Image.
- **Restore:** Starts the Restore Wizard. This guides you through the process of restoring a volume from a backup image file. For more information, see Restoring a Volume.
- **Explore Backup:** Starts the Explore Backup Wizard. This guides you through mounting a backup image file as a volume so you can restore individual files and folders. For more information, see Mounting Backup Image Files.

Management View Tab

The Management View tab is one way to access the remote management capabilities of ShadowProtect. It is the preferred management view for users of ShadowProtect Server and ShadowProtect SBS because it lets you easily manage many nodes from a single location.



	Computer	Connection Status	Last Backup	Next Backup	Backup Failures	Backup Progress
✓	Local Machine (1) Agent Status Good: 1 Failed: 0 Ignored: 0					
✓	DAD	Connected	✓ 3/19/2013 5:00:54 PM	3/19/2013 6:00:00 PM	0	

The Management View tab is divided into two panes: Node Controls and Node List.

Node Controls

The Node Controls pane lets you manage connected nodes using the following controls:

Control	Description
Connect	Connects a previously-added managed remote node to the ShadowProtect user interface.
Disconnect	Disconnects a managed remote node from the ShadowProtect user interface.
Add	Adds a system that has the ShadowProtect Backup Agent installed to the node list.
Delete	Deletes a remote node from the managed node list.
Edit	Opens the Server Details dialog box of the currently selected node (see Modifying Remote Node Properties).
Manage	Opens the ShadowProtect tabs (Disk Map, Backup Jobs, Destinations, Backup History) for the currently selected node.
Install	Opens the ShadowProtect Push Wizard, which lets you push the ShadowProtect agent out to other systems that you want to manage from this Management View. For more information, see Installing the Backup Agent Remotely.

Node List

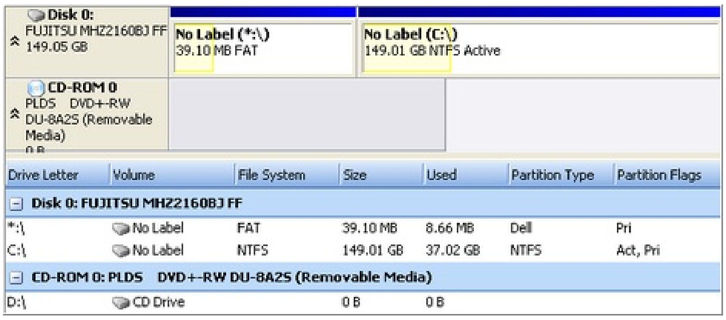
The Node List appears below the Controls pane. This is a list of nodes currently managed by this console with these details.

Column	Description
Computer	Displays the Windows Computer Name for the system.
Connection Status	Identifies if a managed system is currently connected to this console.
Last Backup	Lists the time for the last scheduled backup. A green checkmark indicates the backup succeeded. A red dash indicates a failure.
Next Backup	Shows the time for the next scheduled backup.
Backup Failures	Indicates the number of backup failures for the system.
Backup Progress	Displays the percentage (%) completed of a currently running backup job.
Basic Properties	Each node displays information in three columns: **Job Status:** Displays information about the current backup job, including the destination backup image file, and status (queued, running, completed), and the time remaining (running job) or total time (completed job). Click **View Details** to view the Volume Backup tab. **Backup Job:** Displays information about the backup job configuration, including Compression, Encryption, and the backup job options. **Schedule:** If the selected backup job is a recurring job, the Basic Properties tab displays the job schedule for both Full backup images, and Incremental backup images, where applicable.

Backup Progress	Displays detailed information about the currently running backup job, including time remaining, throughput, and an Event log. If no backup job is running, the Volume Backup tab displays details from the most recent backup job.

Disk Map Tab

The *Disk Map* tab provides a graphical view of available system drives--listing each physical disk drive with its partitions.The Disk Map tab also lets you access the Backup and Restore Wizards for the selected drive.



Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
Disk 0: FUJITSU MHZ2160BJ FF						
*:\	No Label	FAT	39.10 MB	8.66 MB	Dell	Pri
C:\	No Label	NTFS	149.01 GB	37.02 GB	NTFS	Act, Pri
CD-ROM 0: PLDS DVD+-RW DU-8A2S (Removable Media)						
D:\	CD Drive		0 B	0 B		

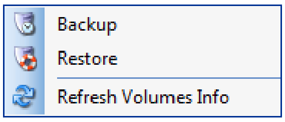
Note: In the Recovery Environment, you can also run Chkdsk, format a drive or edit the selected disk's `boot.ini` file using the Disk Map tab.

Disk Options

Right-click on a disk's description at the left and the Refresh Volumes Info option appears. This option refreshes this disk's volume list.

Partition Options

Right-click a partition entry in Disk Map to open an actions menu for that entry:



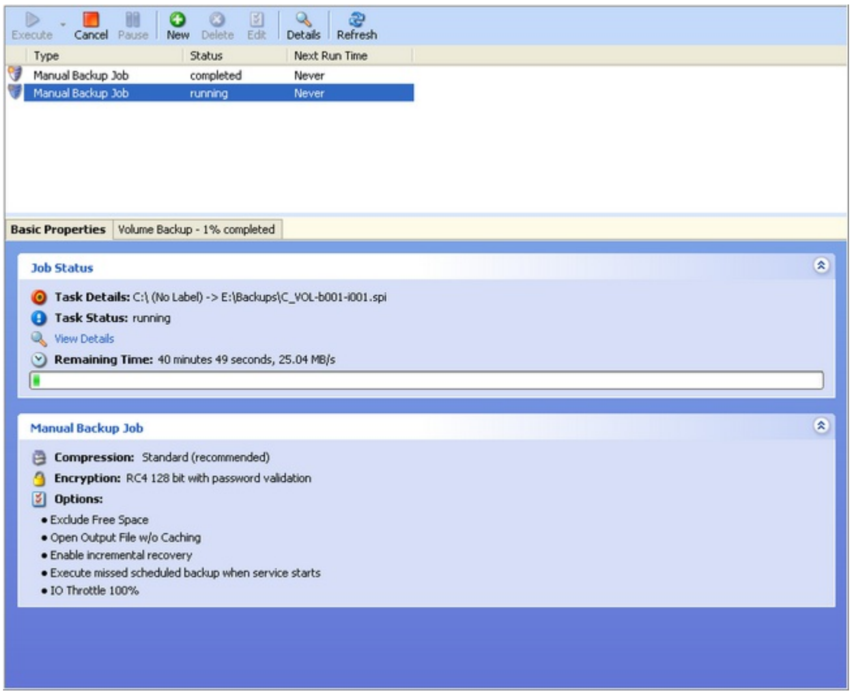
Note: These same options appear when right-clicking on a volume in the list at the bottom of the pane.

These menu options perform these actions:

Option	Description
Backup	Launches the Backup Wizard (see Creating Backup Image Files).
Restore	Launches the Restore Wizard (see Restoring a Volume).
Refresh Volumes Info	Refreshes the ShadowProtect volume list for the current system.

Backup Jobs Tab

The Backup Jobs tab displays scheduled backup jobs. From this tab, you have complete control over the ShadowProtect jobs configured for the current system.



Type	Status	Next Run Time
Manual Backup Job	completed	Never
Manual Backup Job	running	Never

Basic Properties | Volume Backup - 1% completed

Job Status

Task Details: C:\ (No Label) -> E:\Backups\C_VOL-b001-i001.spi

Task Status: running

View Details

Remaining Time: 40 minutes 49 seconds, 25.04 MB/s

Manual Backup Job

Compression: Standard (recommended)

Encryption: RC4 128 bit with password validation

Options:

- Exclude Free Space
- Open Output File w/o Caching
- Enable incremental recovery
- Execute missed scheduled backup when service starts
- IO Throttle 100%

The Backup Jobs tab is divided into two panes and includes a right-click menu:

Job Controls Pane

The upper Job Controls pane lets you manage backup jobs. Select a backup job from the job list to manage it, and view job information in the Job Information pane. The Job Controls pane includes the following controls:

Control	Description
Execute	Immediately executes the next task for the selected backup job--either a full backup or an incremental--depending on if the job creates incrementals or full weekly or monthly backups. **Warning:** Execute includes an arrow to open a menu with Full and Incremental options. (Execute defaults to the job's type.) If the job creates incrementals, ONLY select Full to stop the current backup chain and start a new one.
Cancel	Cancels the selected backup job. This terminates a currently running job, but keeps the job status as enabled (this means that the job executes at its Next Run Time).
Pause	Toggles the selected job status between Enabled and Disabled. A disabled job is suspended and will not run until re-enabled.
New	Launches the Backup Wizard (see Create a Backup Image).
Delete	Deletes the selected job.
Edit	Launches the Backup Wizard, where you can edit the selected job's configuration (see Create a Backup Image).
Details	Opens the Volume Backup tab in the Job Information pane so you can see details about the currently selected backup job.
Refresh	Refreshes the volume information in the Backup Job Information pane.

Job Information

Displayed in the lower pane, Job Information includes two tabs--Basic Properties and Volume Backup--that provide information about the currently selected backup job.

Basic Properties Tab

Displays details on:

Job Status	• Status (queued, running, or completed) • View Details Button (opens the Volume Backup tab) • Time remaining to complete the job (running job) or total time (completed job) • Average data transfer rate in megabytes/second
Scheduled Backup Job	Provides details on the type of backup job: • Compression type (High, Standard, or None) • Encryption (password protect the backup file or not) • Options from the job's configuration such as: --Include or exclude free space from the backup --Performance Throttling (priority of the backup process) --Incremental or full backup
Schedule	Describes when to perform the backup

Volume Backup Tab

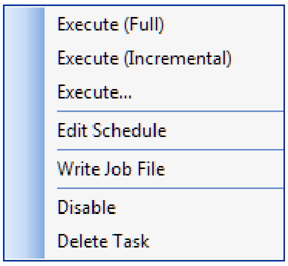
Displays details on:

Status	Completed or Running
Source	Identifies the volume the job backs up
Destination	Identifies where ShadowProtect stores this job's backup image files
Event Log	Displays detailed information about the currently running or the most recent backup job.

Note: Click **Close** to exit the Volume Backup tab.

Right-Click Menu

Select a backup job and right-click on it to display this menu:

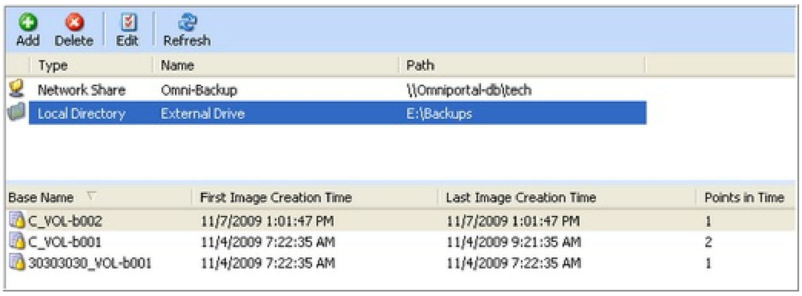


These options include:

Execute (Full)	Immediately starts a new full backup of the selected job's volume. **Caution:** If the selected job creates continuous incrementals, clicking Execute (Full) stops the existing chain and starts a new one with a new full backup file.
Execute (Incremental)	Immediately starts a new incremental of the volume either for incremental or weekly/monthly jobs.
Execute...	Immediately starts a new full backup of the selected job's volume (same as Execute (Full)). **Warning:** If the selected job creates continuous incrementals, clicking **Execute...** stops the existing chain and starts a new one with a full backup file.
Edit Schedule	Modifies the backup job's execution time (for details on the schedule dialog, see Creating Backup Image Files).
Write Job File	Creates a job file in the ShadowProtect\Jobs folder for use by STC Support in troubleshooting.
Disable	Temporarily halts the execution of the selected backup job. (Toggles to *Enable* after selecting *Disable*.)
Delete Task	Deletes the selected job.

Destinations Tab

The Destinations tab shows a list of configured storage locations for backup image files. Use this tab to create or modify destinations used by ShadowProtect backup jobs. For more information see Using Destinations.



Type	Name	Path
Network Share	Omni-Backup	\\Omniportal-db\tech
Local Directory	External Drive	E:\Backups

Base Name	First Image Creation Time	Last Image Creation Time	Points in Time
C_VOL-b002	11/7/2009 1:01:47 PM	11/7/2009 1:01:47 PM	1
C_VOL-b001	11/4/2009 7:22:35 AM	11/4/2009 9:21:35 AM	2
30303030_VOL-b001	11/4/2009 7:22:35 AM	11/4/2009 7:22:35 AM	1

The Destinations tab includes:

Menu Bar

This offers options for working with destinations:

Add Opens the Destination dialog box.

Delete Deletes the currently selected Destination.

Edit Opens the Destination dialog box so you can modify the existing configuration (see Editing Destinations).

Refresh Updates the Destination Objects List and the Destination Objects Information List.

Destinations List

This upper pane displays a list of currently defined destinations for image files. Select a destination to view Information about the backup image sets stored there. Use the menu bar to perform another operation. The list shows:

Type Identifies the destination as a Local Directory or a Network Share.

Name Shows the name given the destination when it was created.

Path Displays the network path or drive letter\volume\folder to the destination.

Image Sets

The lower pane displays information about the backup image sets stored in the currently selected destination. This includes:

Base image file name The name of the first file--a full image of the volume--in the backup incremental chain.

First image creation time The ShadowProtect date and time stamp of the base image file

Last image creation time The ShadowProtect date and time stamp of the last incremental in that chain.

Points in Time The number of incrementals stored in this backup chain.

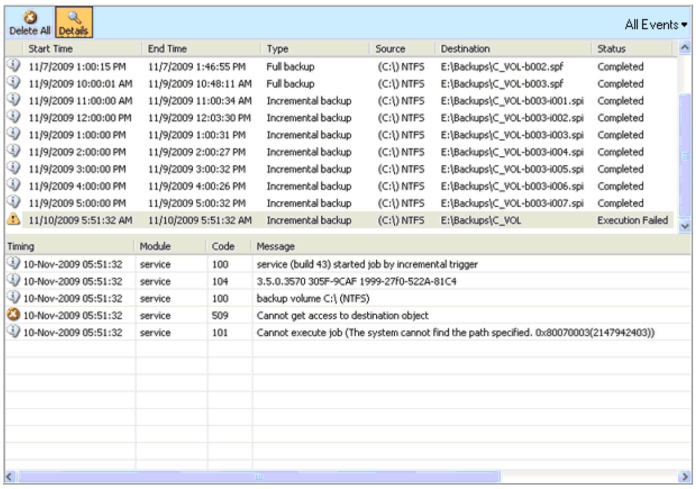
Image List Doesn't Update

When ShadowProtect or ImageManager adds image files to a network destination (such as a NAS device), the list of these files under the Destination tab may not update automatically. Use **Refresh** to update the list.

This most often occurs with Linux-based NAS devices as they do not always send out update notifications to ShadowProtect.

Backup History Tab

The Backup History tab displays the backup job log:



	Start Time	End Time	Type	Source	Destination	Status
ⓘ	11/7/2009 1:00:15 PM	11/7/2009 1:46:55 PM	Full backup	(C:\) NTFS	E:\Backups\C_VOL-b002.spf	Completed
ⓘ	11/9/2009 10:00:01 AM	11/9/2009 10:48:11 AM	Full backup	(C:\) NTFS	E:\Backups\C_VOL-b003.spf	Completed
ⓘ	11/9/2009 11:00:00 AM	11/9/2009 11:00:34 AM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i001.spi	Completed
ⓘ	11/9/2009 12:00:00 PM	11/9/2009 12:03:30 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i002.spi	Completed
ⓘ	11/9/2009 1:00:00 PM	11/9/2009 1:00:31 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i003.spi	Completed
ⓘ	11/9/2009 2:00:00 PM	11/9/2009 2:00:27 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i004.spi	Completed
ⓘ	11/9/2009 3:00:00 PM	11/9/2009 3:00:32 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i005.spi	Completed
ⓘ	11/9/2009 4:00:00 PM	11/9/2009 4:00:26 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i006.spi	Completed
ⓘ	11/9/2009 5:00:00 PM	11/9/2009 5:00:32 PM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL-b003-i007.spi	Completed
⚠	11/10/2009 5:51:32 AM	11/10/2009 5:51:32 AM	Incremental backup	(C:\) NTFS	E:\Backups\C_VOL	Execution Failed

Timing	Module	Code	Message
ⓘ 10-Nov-2009 05:51:32	service	100	service (build 43) started job by incremental trigger
ⓘ 10-Nov-2009 05:51:32	service	104	3.5.0.3570 305F-9CAF 1999-27f0-522A-81C4
ⓘ 10-Nov-2009 05:51:32	service	100	backup volume C:\ (NTFS)
✖ 10-Nov-2009 05:51:32	service	509	Cannot get access to destination object
ⓘ 10-Nov-2009 05:51:32	service	101	Cannot execute job (The system cannot find the path specified. 0x80070003(2147942403))

The Backup History tab shows:

Menu Bar

The menu offers:

Delete All	Clears the Job List log file.
Details	Displays or hides the Job Log pane.
Status Filter	The filter is a dropdown menu at the right side of the menu bar. This opens a sub-menu with options to filter the backup jobs to show All, Completed, Aborted, or Failed jobs. The default is All Events.

Job History

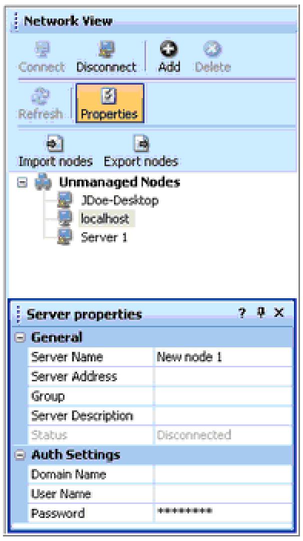
The upper pane displays a list of past backup jobs. Select a job to view job details in the Job Log. You can sort the backup history lists using the column headers. You can also adjust the column width by dragging the column header borders.

Job Log

The lower pane displays the log entries for the selected job. (**Note:** This is the same information available in the Volume Backup tab.) These entries help in troubleshooting issues with backups.

4.4 Network View

The Network view displays information for managing ShadowProtect on remote systems (see Remote Management). Select Network View from the Navigation panel to see this panel while viewing any of the tabs.



Server properties

General	
Server Name	New node 1
Server Address	
Group	
Server Description	
Status	Disconnected
Auth Settings	
Domain Name	
User Name	
Password	********

The Network View includes the following controls:

Control	Description
Connect	Connects the ShadowProtect console to a previously added, managed remote node.
Disconnect	Disconnects a managed remote node from the ShadowProtect console.
Add	Adds a system to the node list. This system must have the ShadowProtect backup agent installed.
Delete	Deletes a remote node from the managed node list.
Refresh	Refreshes the remote node list.
Properties	Toggles the Properties table on and off.
Import Nodes	Imports a previously exported node list into your Network View.
Export Nodes	Exports your node list into an XML file.

Properties Table

This table shows:

General	Displays details of the selected node: • Server Name--Shows the Windows machine name for the node. • Server Address--Repeats the machine name if local, the address if remote. • Group name--Shows which group the system is part of. • Server Description--Indicates if the node is local or remote. • Status--Displays the connection status of the node to this ShadowProtect console.
Auth Settings	Displays the authentication details for the selected node: • Domain name--Indicates the network domain name if a remote node. • User name--Displays the user name used to log into a remote node. • Password--Indicates the password used to log into the remote node.
Agent Information	Displays details of the node's ShadowProtect agent: • Agent version--Shows the installed version of the ShadowProtect agent. • Last connected--Indicates the date and time this node was last connected to this console.

5 Creating Backup Image Files

Note: For information about creating a backup image file in Recovery Environment, see the *StorageCraft Recovery Environment User Guide*.

ShadowProtect provides two ways to create backup image files using the Backup Wizard:

One-Time Backup: The Backup Wizard guides you through creating an immediate full backup image file. Consider the following when creating a one-time backup job:

- ShadowProtect supports one-time backup images from both Windows and Recovery Environment. For more information about each of these products, see Features and Components.
- You must be a member of the Administrator group on the system where you want to create a backup.
- One-time backup jobs can be run at any time. They do not affect existing scheduled backup jobs for that volume.

Scheduled Backup: The Backup Wizard guides you through the process of creating a recurring backup job. Consider the following when creating a scheduled backup job:

- A volume can belong to no more than one scheduled incremental backup job. Note that this limitation does not prevent creating a one-time backup image or a differential backup image of that volume.
- If ShadowProtect is currently running a backup job for that volume, or the computer is turned off and unavailable,

ShadowProtect skips any scheduled backup jobs for that volume at that time.
- ShadowProtect supports scheduled backup images only from Windows (not the Recovery Environment).
- ShadowProtect includes VirtualBoot, which allows administrators to launch a temporary replacement for a crashed or disabled server or workstation **Note**: In order to continue the existing backup chain for the system while it is hosted on a VirtualBoot VM, you *must* use a ShadowProtect Destination Object of type "Network Share" in the backup job to store the system's image files (see Destinations).

Note: Use the Backup Wizard to configure a NETGEAR ReadyDATA destination.

Backup Scheduling Options

ShadowProtect offers a set of scheduling options:

Now

- Creates Full or Differential backup images.
  Note: The differential option is active only for an existing chain.
- Creates a one-time backup job that starts as soon as the Backup Wizard closes.

Later

- Creates full backup images.
- Creates a one-time backup job at the specified date and time.

By default, the Start Time fields display the current date and time. To change the date and time settings, click on an element of the date/time (month, day, year, hour minute, second, AM/PM), then type or use the up/down buttons to set the desired value.

Weekly

- Creates Full and Incremental backup images.
- Creates a recurring backup job based on a weekly schedule. You select the weekdays and time of day to start a Full backup.
- Optionally, you can specify a schedule for Incremental backups.

  a. Select the weekdays to create incremental backups.
  b. Specify times of day to start and stop creating incremental backups.
  c. Specify the incremental backup frequency (minutes between incremental backups).

Note: The Weekly schedule always creates a new full backup at least once a week, even after the incrementals in between. To create a backup job that takes a full backup and then a single incremental once a week, for example, select *Continuous Incrementals* and define the day and time to take the incremental once a week. For example, select only Saturday for an incremental, with the interval of 999 minutes. This creates a single full backup at the start of the job, then a single incremental on Saturday each week. In the event of a drive failure, however, such a schedule would result in the loss of up to a full week of data.

Monthly

- Creates Full and Incremental backup images.
- Creates a recurring backup job based on a monthly schedule. Select the days of the month and time of day to start a full backup.
- Optionally, you can specify a schedule for incremental backups.

  a. Select the weekdays to create incremental backups.
  b. Specify times of day to start creating incremental backups

Continuous Incrementals

- Creates Full and Incremental backup images.
- Creates a single Full backup, then creates recurring incremental backups from that point forward. This option requires StorageCraft ImageManager (see the *StorageCraft ImageManager User Guide*).

To specify the Incremental backup schedule:

a. Select the weekdays to create incremental backups.
b. Specify times of day to start and stop creating incremental backups.
c. Specify the Incremental backup frequency (minutes between incremental backups).

Note: ShadowProtect allows only one incremental backup job for each source volume.

Creating a Differential Backup Image

Use a differential to create a backup file that contains only the differences since the last backup. Note that a To create a differential:

1. Select Differential backup in the wizard's *Backup Schedule* page.
2. Continue with the wizard to the *Previous Backup Image* page.
3. Select the existing backup image file to use as a basis for creating the differential backup image.
4. Click **Next**.
5. On the *Options* page, select the desired backup image file options.
   Note: The Options page lets you set both basic and advanced backup image options.
6. Click **Next** to continue with the wizard.
   ShadowProtect creates a differential backup image file for this system.

Email Notifications

To receive email notifications when a backup job succeeds or fails, go to **Options** > **Agent Options**. Configure an email address, then select either or both *Send Email on Success* or *Send Email on Failure* to receive notices.

Start a New Job after an OS Upgrade

Operating system upgrades make profound changes to software. StorageCraft recommends starting a new backup job after an OS upgrade rather than attempt to continue with an older existing chain of the same volume. If the upgrade is from one major OS release to another, you will also need to deactivate the ShadowProtect license and uninstall the software prior to the upgrade. (For example, a major upgrade would be from a Windows 7 system to Windows 8 or a Windows 8 to Windows Pro.) After the OS upgrade, reinstall ShadowProtect and reactivate the license.

Note: The system preserves backup job configurations and other ShadowProtect settings through the reinstall.

5.1 Backup Image File Storage Locations

ShadowProtect can store backup image files on any disk device:

- Hard drives
- Removeable USB/FireWire drives
- Network drives
- Network Attached Storage (NAS) devices.

and optical media:

- CDs
- DVDs
- Blu-Ray discs

Each has advantages and disadvantages:

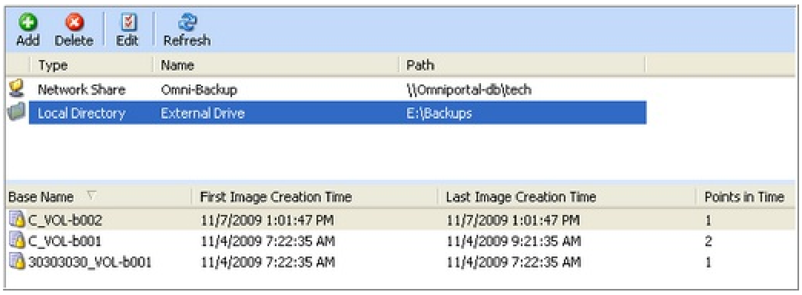
Location	Advantages	Disadvantages
Local Hard Drive	• Fast backup and restore • Inexpensive	• Consumes local disk space • Vulnerable to loss if the drive fails • Cannot use the source drive or volume as the target for backups
Local USB/FireWire Drive	• Fast backup and restore • Preserves disk space on local drives • Inexpensive • Easy off-site storage	• More expensive than local hard drives • Vulnerable to loss if the drive fails

Network Hard Drive (Server)	• Fast backup and restore • Protection from local hard drive failure • Off-site storage • Can run ImageManager on system	• Must have network interface card drivers supported by Recovery Environment • Complexity. Users must have network rights to save and access backup images
Network Attached Storage (NAS)	• Relatively fast backup and restore • Protection from local drive failure • Preserves local disk space	• Must have network access to reach device • Must have access rights to the device
Optical (CD/DVD/Blu-Ray)	• Good media for archiving • Protection from local hard drive failure	• Slower backups due to media speeds vs. hard drives • File restrictions due to limited capacity of discs • Spanning large files over multiple discs adds management effort

⚠ **Note**: If you select a destination that does not have enough disk space to save the backup image, the backup job fails. ShadowProtect notes the reason for the failure in its log file (and in the Backup History tab).

5.2 Destinations

Backup destinations are pre-defined storage locations for backup image files. ShadowProtect supports both local and network storage as destinations. If a destination storage device changes, you only have to modify the destinations that point to that storage device, rather than edit all backup jobs which use that destination.



Type	Name	Path
Network Share	Omni-Backup	\\Omniportal-db\tech
Local Directory	External Drive	E:\Backups

Base Name	First Image Creation Time	Last Image Creation Time	Points in Time
C_VOL-b002	11/7/2009 1:01:47 PM	11/7/2009 1:01:47 PM	1
C_VOL-b001	11/4/2009 7:22:35 AM	11/4/2009 9:21:35 AM	2
30303030_VOL-b001	11/4/2009 7:22:35 AM	11/4/2009 7:22:35 AM	1

⚠ **Note:** Destinations can point to only one folder. StorageCraft strongly recommends that each system have a unique folder to store its image files since mixing these files from different systems makes it almost impossible to manage. As a result, you must define a different destination for each system. However, you can use this one destination folder to save all the backup jobs from the same system. (For example, if the system has multiple volumes such as a boot volume and a data volume.)

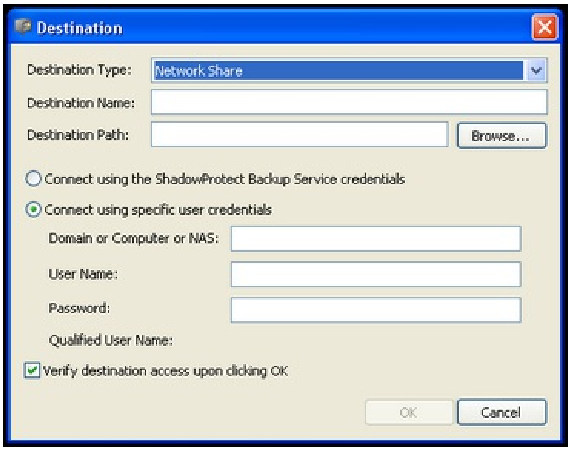
Using a Windows Dedup Volume as a Destination

ShadowProtect supports writing backup image files to a Windows Dedup-enabled volume. However, since ShadowProtect compresses image files, Windows Dedup does not yield significant space savings. Also, if any of the dependent backup files in the backup chain are deduped, ShadowProtect cannot:

- Mount the backup file
- Run a VirtualBoot on the backup file.

To create a backup job destination

1. Open the ShadowProtect console, then select **Tasks** > **Add Destination**.
   This displays the Destinations dialog box. You can also open the Destinations dialog box from the Backup Name and Destination page of the Backup Wizard (see Creating Backup Image Files).



Destination

Destination Type: Network Share

Destination Name:

Destination Path: Browse...

○ Connect using the ShadowProtect Backup Service credentials

● Connect using specific user credentials

Domain or Computer or NAS:

User Name:

Password:

Qualified User Name:

☑ Verify destination access upon clicking OK

2. Specify the settings for the new destination, then click **OK**.

Destination Type

Select the type of destination to create:
Local Directory: The destination is on a locally connected storage device (HDD, USB drive, etc.)
Network Share: The destination is on the network.
Note: Select a "Network Share" Destination Type to continue the backup chain even if the source system itself suffers a failure. Choosing a Network Share allows users to launch a VirtualBoot temporary replacement for the failed system.

Destination Name

Specify a descriptive name for this destination.

Destination Path

Click **Browse** to locate the destination.
Local Directory: Click **Browse**, then select the local drive and folder to store backup images.
Network Share: Click **Browse**, then select the network location to store backup images.

⛔ **Warning:**The Destination Path cannot contain special characters:

` ! @ # $ % ^ & * ( ) | \/ ? > < , { } [ ]

The path also cannot exceed 186 characters in length. If either occurs, the connection fails.
⛔ **Warning:** Do not change the Network Share name using a Windows utility or the Management page in a NETGEAR ReadyDATA NAS. Doing so causes the job to fail.

User Credentials

Specify the credentials needed:
Network Share: Enter the network credentials.
ShadowProtect Backup Service credentials: Use the same stored credentials used by the ShadowProtect backup service to access your system.
Specific user credentials: Provide the Container (Domain, Computer name, or NAS device name), Username and Password that ShadowProtect should use to access this network share.

Verify Destination Access

Instructs ShadowProtect to verify the destination path and access credentials, if necessary, before creating the destination.
If the destination access verification is not successful, the program alerts you that it could not create the destination. If this happens, confirm the path and credentials are accurate, then re-create the destination.

Netgear ReadyDATA Destinations

The configuration of a Netgear ReadyDATA system as a backup file target destination uses the *Backup Wizard*, not the Desitnations tab.

Editing Destinations

To edit a backup job destination

1. Start the ShadowProtect Console (see Starting ShadowProtect).
2. Select the Destinations tab.
3. Select the destination to edit, then click **Edit**.
This opens the Destination dialog box showing the current destination configuration. From this dialog box, you can edit all of the destination's properties except the Destination Type (Network Share or Local Directory). If this type changes, create a new destination.

Deleting Destinations

To delete a backup job destination

1. Start the ShadowProtect console (see Starting ShadowProtect).
2. Select the Destinations tab.
3. Select the destination to delete, then click **Delete**.

   ⚠ Note: Before deleting a destination, make sure to modify or delete any backup jobs that use the destination or the jobs will fail. For information about editing backup jobs, (see Backup Jobs Tab.)

5.3 Configuring a Continuous Incremental Backup Job

A continuous incremental backup job creates:

- An initial single full backup (base image)
- Recurring incremental backups from that point on at set intervals.

Incremental backups benefit from using StorageCraft ImageManager to manage the amount of disk space used by the files and to maintain their integrity.

Some points to consider when configuring a continuous incremental backup job**:**

- Provide a name for the backup job. While ShadowProtect does not require a user-defined name, creating a unique name allows quick identification of related backup files in a folder. ShadowControl CMD also can display the backup job name--again making it easier to determine which job applies to which EndPoint.
- The minimum interval for backups is every 15 minutes. The maximum is once every 1440 minutes (24 hours). The Wizard will calculate and display the number of backups ShadowProtect will do each day based on the start/stop times and the interval.
- StorageCraft recommends to always use VSS for backups, so leave the *Use VSS* option and the *Sunday* option under *VSS Incremental Backups* section checkmarked. (See *Using VSS* for details on when to not use VSS.)
- StorageCraft also strongly recommends using the free StorageCraft ImageManager software to consolidate backup files. A continuous incremental job creates an ongoing flow of new files which can quickly saturate a destination drive. To avoid this, use ImageManager to schedule consolidation of older incremental backup files.

System Reserve and other Volumes

Hardware vendors may configure their hard drives to include additional partitions:

- *Diagnostic Partition*: Usually a 100MB or less partition, this would include one or more tools specific to that hardware platform. This partition will have no drive letter assigned to it.
- *Recovery Partition*: Usually a 1GB or less partition, this stores data existing on the boot partition prior to installing the Operating System. The Recovery Partition is used to restore the system back to factory default status.This partition will have no drive letter assigned to it.
- *System Reserve Volume*: This may include boot information and is of particular value only when using Microsoft Windows BitLocker.

A ShadowProtect restore typically does not require a backup of any of these volumes. Instead ShadowProtect:

- Recreates the boot information from the System Reserve volume during a restore.
- Does not need additional hardware-specific diagnostic tools in the Diagnostic Partition as a typical restore is to new, different hardware.
- Does not need the factory content from the Recovery Partition as this partition contains hardware-specific diagnostic tools not compatible with new, different hardware.

The only exception is in the case of a system which uses Windows BitLocker to encrypt a partition. If a user uses the Recovery Environment to create a full cold backup of the encrypted partition, a one-time full backup of the System Reserve volume is required. This one-time backup preserves the Bitlocker data required to decrypt the partition.

Note that user-preference may warrant preserving these partitions with one-time full backups.

GPT Disk Volumes

GPT disks also include additional volumes:

- the EFI System partition (ESP)
- the Microsoft Reserved Partition (MSR)

Neither of these require a backup, as ShadowProtect automatically restores the required partitions during recovery. (In fact, the MSR contains no file system to back up.)

Creating a Continuous Incremental Backup Using the NETGEAR ReadyDATA

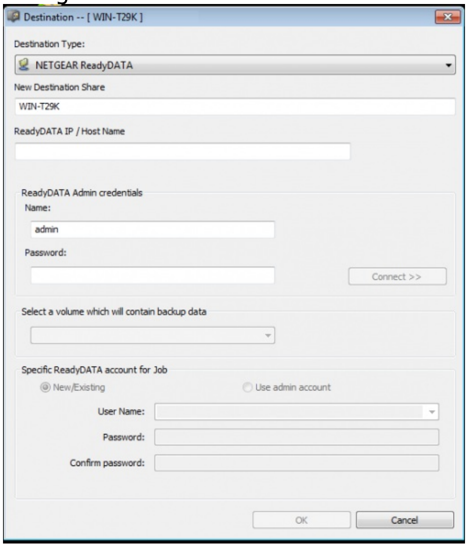
ShadowProtect 5.2.0 and StorageCraft Recovery Environment for Windows now support the NETGEAR ReadyDATA system. The procedure in configuring and using the NETGEAR ReadyDATA differs from the standard procedure. This section describes these considerations.

Considerations when using the NETGEAR system:

- It is defined as a destination using the Backup Wizard, *not* the Destinations tab as with most network resources.
- It exclusively supports continuous incremental backup jobs.
- Its backups are automatically saved as vhdx-format virtual disks.
- It includes a unique backup file retention policy run by ShadowProtect for the ReadyDATA system. (Incremental backup jobs using any other destination rely on StorageCraft ImageManager to implement retention policies.)

To configure a NETGEAR ReadyDATA destination:

1. In the Backup Wizard's *Backup Name and Destination* dialog, select *Network Locations* in the location dropdown box. The *Destination* dialog opens.
2. In the Destination Type dropdown box, select *NETGEAR ReadyDATA*. The dialog changes to reflect the NETGEAR configuration:



Destination -- [WIN-T29K]

Destination Type: NETGEAR ReadyDATA

New Destination Share: WIN-T29K

ReadyDATA IP / Host Name:

ReadyDATA Admin credentials

Name: admin

Password:

Select a volume which will contain backup data

Specific ReadyDATA account for Job

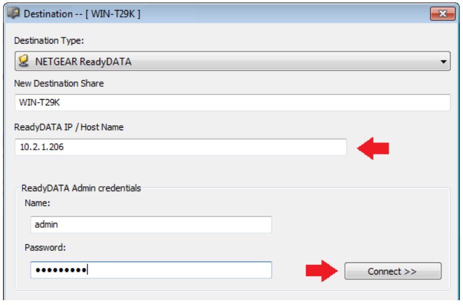
● New/Existing ○ Use admin account

User Name:

Password:

Confirm password:

3. Enter a unique Destination Share name.
   Warning: Do not change the Destination Share name later on using a Windows utility or the Management page in a NETGEAR ReadyDATA NAS. Doing so causes the job to fail. Attempting to recreate the job using the same Share name also results in an error.
4. Enter the IP address (or device name) and login credentials for the NETGEAR ReadyDATA system:



Destination -- [WIN-T29K]

Destination Type: NETGEAR ReadyDATA

New Destination Share: WIN-T29K

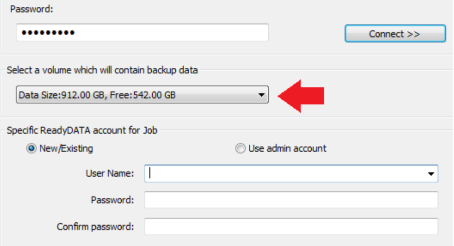
ReadyDATA IP / Host Name: 10.2.1.206

ReadyDATA Admin credentials

Name: admin

Password: •••••••••

5. Click **Connect**. ShadowProtect displays volume information for the NETGEAR system after successfully connecting.



Password: •••••••••

Select a volume which will contain backup data: Data Size:912.00 GB, Free:542.00 GB

Specific ReadyDATA account for Job

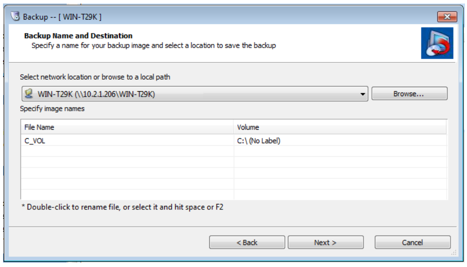
● New/Existing ○ Use admin account

User Name:

Password:

Confirm password:

6. Select either *New/Existing* or *Use admin account* to run the job. Use *New/Existing* to select an existing NETGEAR user or create a new one to run the job. (ShadowProtect automatically creates the user on the NETGEAR when specifying a new user.) Select *Use admin account* to use that account to run the job.
7. Click **OK** to save the configuration. ShadowProtect displays the *Backup Name and Destination* dialog again, now showing the NETGEAR destination in the location box:



Backup -- [WIN-T29K]

Backup Name and Destination
Specify a name for your backup image and select a location to save the backup

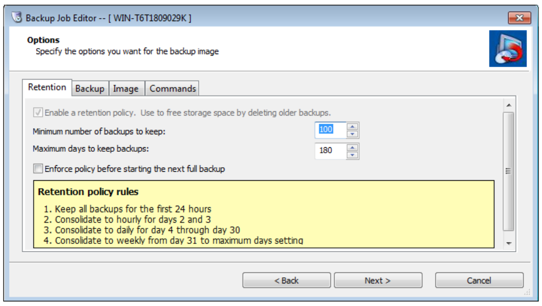
Select network location or browse to a local path: WIN-T29K (\\10.2.1.206\WIN-T29K)

Specify image names

File Name	Volume
C_VOL	C:\ (No Label)

* Double-click to rename file, or select it and hit space or F2

8. Click **Next**. ShadowProtect displays the Backup Job Editor showing the Retention Policy Rules. (**Note:** This is different than regular continuous incremental backup jobs which rely on ImageManager to configure retention policy.) These rules describe how the NETGEAR consolidates and removes older backups.



Options
Specify the options you want for the backup image

☑ Enable a retention policy. Use to free storage space by deleting older backups.
Minimum number of backups to keep: 100
Maximum days to keep backups: 180
☐ Enforce policy before starting the next full backup

Retention policy rules
1. Keep all backups for the first 24 hours
2. Consolidate to hourly for days 2 and 3
3. Consolidate to daily for day 4 through day 30
4. Consolidate to weekly from day 31 to maximum days setting

9. Select the minimum number of backups to keep and the maximum number of days to keep those backups.
10. Select *Enforce policy before starting the next full backup* to have ShadowProtect consolidate or delete backups prior to running the next backup. This conserves space and prevents a possible failed backup in the event of the drive running out of space. If the Enforce policy option is left unchecked, the NETGEAR system executes the backup, then performs any retention policy events.
11. Click **Next** to continue configuring the backup job as outlined for other continuous incremental jobs.

Using VSS

ShadowProtect uses the Windows VSS framework to provide consistent backups of SQLServer, Exchange, Active Directory, Oracle or other database systems. VSS ensures that all cached data is written to disk prior to taking the snapshot. Using VSS, ShadowProtect simplifies a system restore--whether on a server or a workstation. For these reasons, using VSS is the default for all ShadowProtect backup jobs.

There are, however, a few uncommon scenarios where taking a non-VSS backup may be an option:

- One or more VSS components fail, causing the backup job to fail.
- Limited disk space requires smaller incremental file sizes.
- Limited server resources (RAM or CPU) requires a simpler backup operation.

The preferred solution to these issues is to either resolve the failure or provide additional storage or processor resources. However, it is possible to configure a backup job to run wthout VSS or to only use VSS on set occasions.

Note: The option to use or not use VSS is only available when configuring a continuous incremental backup job.

This table summarizes strategies for various backup issues:

Issue	Possible Resolutions
VSS component failure	Some VSS writers do not fully or correctly comply with the VSS spec. This may cause VSS to halt. This type of error will be noted in the backup job's log file. Refer to the Agent Options page for details on using VSS Options to resolve this problem.
Limited disk space	This may occur with a NAS destination for multiple systems' backup files. Rather than have a backup fail for lack of space, configure ShadowProtect to take a non-VSS backup. The resulting non-VSS incremental file typically gives a modest decrease in size compared to a full VSS backup. This decrease may be useful then for multiple devices to continue to backup to a single volume until more space becomes available.

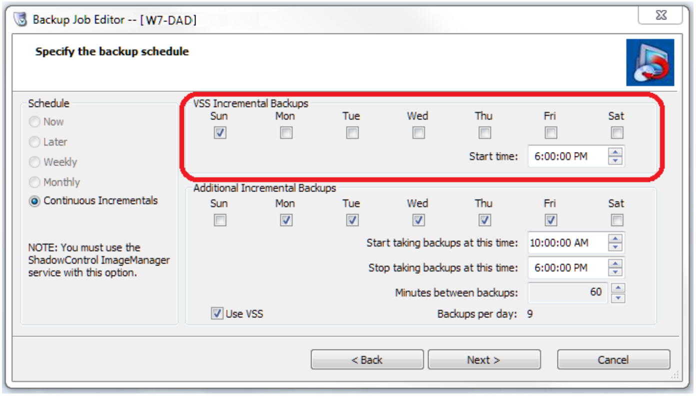
Limited server resources	A server may host multiple processor-intensive applications (such as may occur with Windows SBS). Adding the task of executing an incremental backup every 15 minutes may result in poor performance. Opting for a non-VSS backup could limit the impact of each snapshot on the server. Rather than execute non-VSS backups only, the recommendation is to configure the job to executle non-VSS backups during business hours, then execute a VSS backup after hours.

Non-VSS-Aware Applications

Some applications, such as Intuit QuickBooks, remain non-VSS-aware. These applications may seem like a good case to configure a non-VSS backup. However, it is not. Instead, ShadowProtect supports both pre- and post-backup scripts which can run commands to stop and restart these non-VSS-aware apps. (See Commands for details on running scripts.)

Configuring a Scheduled VSS Backup Job

The Backup Job wizard can configure a scheduled backup job using VSS on one or more days. Use the *VSS Incremental Backups* section of the **Backup Schedule** dialog:



Backup Job Editor -- [W7-DAD]

Specify the backup schedule

Schedule
○ Now
○ Later
○ Weekly
○ Monthly
● Continuous Incrementals

NOTE: You must use the ShadowControl ImageManager service with this option.

VSS Incremental Backups

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☑	□	□	□	□	□	□

Start time: 6:00:00 PM

Additional Incremental Backups

Sun	Mon	Tue	Wed	Thu	Fri	Sat
□	☑	☑	☑	☑	☑	□

Start taking backups at this time: 10:00:00 AM

Stop taking backups at this time: 6:00:00 PM

Minutes between backups: 60

☑ Use VSS

Backups per day: 9

To configure this job:

1. Mark the day(s) to perform the VSS backup.
2. Use the combo box to specify the time to run the VSS job.

   Note: If the aim is to reduce the workload on a server, select a time after business hours.

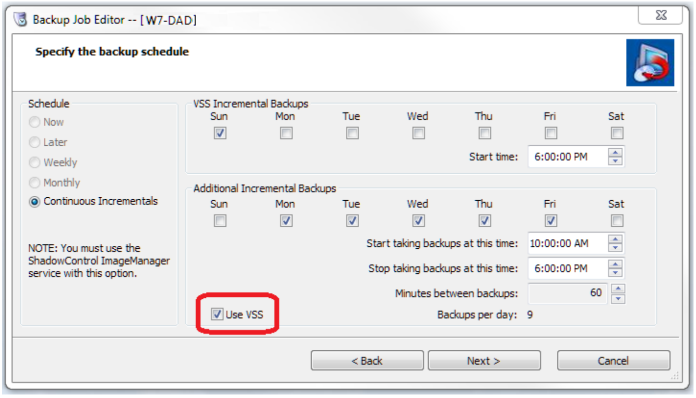
3. Uncheck **Use VSS** in the lower *Additional Incremental Backups* section.

   Note: Leaving the **Use VSS** checkbox marked causes ShadowProtect to ignore any settings in the upper VSS Incremental Backups pane. Instead, ShadowProtect uses VSS for all incremental snapshots.

When using both types of backups for a job, ShadowProtect keeps the scheduled VSS backup incremental file in the correct time sequence of the backup job's chain along with the non-VSS backups. In the event of a system restore, select the VSS backup file if possible to ensure a clean restore of the volume rather than selecting one of the non-VSS backups.

Configuring a Non-VSS Backup Job

Use the Backup Schedule dialog to configure a job that only runs non-VSS backups:



Backup Job Editor -- [W7-DAD]

Specify the backup schedule

Schedule
○ Now
○ Later
○ Weekly
○ Monthly
● Continuous Incrementals

NOTE: You must use the ShadowControl ImageManager service with this option.

VSS Incremental Backups
Sun ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □
Start time: 6:00:00 PM

Additional Incremental Backups
Sun □ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □
Start taking backups at this time: 10:00:00 AM
Stop taking backups at this time: 6:00:00 PM
Minutes between backups: 60
☑ Use VSS
Backups per day: 9

1. Uncheck **Use VSS** in the lower *Additional Incremental Backups* section.

2. Uncheck **Sun** (and any other marked days) in the upper *VSS Incremental Backups* section.

Warning: Consider carefully before creating a non-VSS-only continuous incremental backup job. Without VSS, there is the potential for lost data and corrupted files particularly with VSS-aware apps. This type of backup is referred to as "crash-consistent", as it is similar to taking a backup after a power failure on the system. In the event of a restore, these applications may require an extended recovery using the application's tools to repair any losses or corruption. These are the same steps as would be required to recover from system crash--such as a power failure or from an improper shutdown of the application.

5.4 Configuring a Weekly/Monthly Backup Job

The ShadowProtect Backup Wizard guides you through the process of creating a weekly or monthly backup job. Consider the following when creating such a job:

- ShadowProtect creates a separate backup file for each volume.
- The selected backup schedule determines the available backup image types. For more information about these types, see the Glossary.
- ShadowProtect supports differential backup images which save only the changes since the last full backup.
- ShadowProtect can schedule jobs for:

Now
Creates a one-time full (complete volume) or differential (only the changes since the last backup) images.
Starts as soon as the Backup Wizard closes.

Later
Creates a one-time full backup image.
Starts at the specified date and time.
By default, the Start Time fields display the current date and time. To change the date and time settings, click on an element of the date/time (month, day, year, hour minute, second, AM/PM), then type or use the up/down buttons to set the desired value.

Weekly
Creates full or full with incremental backup images.
Creates a recurring backup job based on a weekly schedule.
Select the weekdays and time of day to run the full or full and incremental backups.

Monthly
Creates full or full and incremental backup images.
Creates a recurring backup job based on a monthly schedule.
Select the days of the month and time of day to start the full or full and incremental backups.

System Reserve and other Volumes

Hardware vendors may configure their hard drives to include multiple partitions:

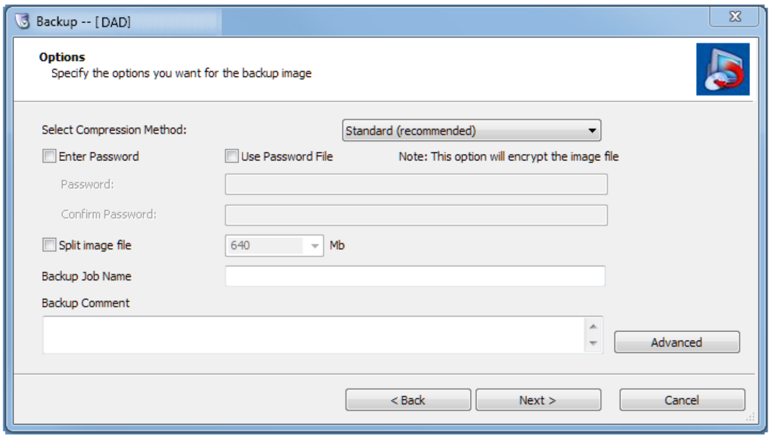
- *Diagnostic Partition*: Usually a 100MB or less partition, this would include one or more tools specific to that hardware platform. This partition will have no drive letter assigned to it.
- *Recovery Partition*: This has only the data included on the new disk prior to installing the Operating System. It is used to restore the system back to factory status. This partition will have no drive letter assigned to it.
- *System Reserve Volume*: This may include boot information and is of particular value only when using BitLocker.

A ShadowProtect restore does not require either a full or continuous backups of these volumes, as it:

- Can recreate the boot information from the System Reserve volume.
- Does not need the factory content from the Recovery Partition since a typical restore occurs after the drive has failed.
- Does not need additional hardware-specific diagnostic tools as again a typical restore is to new, different hardware.

The only exception is in the case of a system using BitLocker. In which case, a one-time full backup of the System Reserve volume preserves the needed content for a full restore. However, user-preference may warrant preserving these volumes with additional one-time full backups.

5.5 Options



Backup -- [DAD]

Options
Specify the options you want for the backup image

Select Compression Method: Standard (recommended)

□ Enter Password □ Use Password File Note: This option will encrypt the image file

Password:

Confirm Password:

□ Split image file 640 Mb

Backup Job Name

Backup Comment

ShadowProtect provides the following backup image file options when creating a backup job:

- Compression Method
- Encryption
- Split Image File
- Backup Comment
- Advanced Options

Note: StorageCraft recommends keeping the default settings for these options. However, the linked sections on each option explain the ramifications of modifying each option if required.

Compression Method

ShadowProtect provides the following file compression options when creating a backup image file:

None	No data compression. This option uses the fewest CPU resources but uses the most disk space.
Standard	Typically compresses data by about 40%. Standard compression provides an optimal balance between CPU usage and disk space usage.
High	Typically compresses data by about 50%. This option requires the most CPU resources, but is useful when disk space is limited.

Contemporary standalone or VM host hardware provides adequate support for the high compression setting. Modify the setting only when extended monitoring reveals performance degradation during backup operations.

File Protection

ShadowProtect provides the following file protection mechanisms for image files. File protection is particularly useful when storing backup image files on a network or replicating off-site to help prevent unauthorized access to the files.

Password Protection: Assigning a password requires the use of the correct password to access the backup image file. Use these guidelines to create a password using ShadowProtect:

- Use a variety of alphanumeric and symbol characters.

- Use a random mixture of characters: upper and lower case letters, symbols and numbers.
- Use at least eight characters.
- Don’t use a word found in the dictionary.
- Once defined, ShadowProtect cannot change the password for a given chain. If changing the encryption password becomes necessary, create a new backup job and chain with the new password.

  Warning: Guard encryption passwords carefully. ShadowProtect cannot access a backup image file without the password. ShadowProtect cannot change passwords on existing encrypted files. Nor can StorageCraft Support recover the password or otherwise provide access to an encrypted backup image file.

File Encryption: ShadowProtect uses the password as an encryption key when encrypting the backup image file. You can select one of three encryption methods in the Advanced Options dialog box. For details, see "Encryption" in Advanced Options.

Use Password File: You can use a password file, also known as a Key File, to encrypt a backup image. This is helpful if you are not managing your own backups and you don’t want other users to have access to the password used to protect the backup image files. For information about creating a Key File, see Creating Key Files.

Important: StorageCraft strongly recommends encrypting all backup files replicated to remote sites.

Split Image File

ShadowProtect can split a large backup image file into multiple smaller files, These smaller files create a *Spanned Image Set*. Use spanned image sets to move a large backup image file onto fixed-length media such as CDs or DVDs.

To split a backup image file:

1. Select **Split Image File** in the Backup Wizard's *Options* page.

2. Specify the maximum file size (in MB) for each of the smaller files in the set the **Split Image File** field. For example, 700MB for CD-Rs or 4000MB for DVD-R.

Note: You can also split an existing backup image file using the Image Conversion Tool.

Note: If a backup image file is divided into multiple files, the filename suffix will change to `.sp1, .sp2, ..., .spN`, where *N* represents the file's sequence within the Spanned Image Set.

Backup Job Name

The Backup Job Name field specifies a name for the job. ShadowProtect uses this name as a prefix for each backup image file created as part of this job. This makes tracking and managing image files simpler. For example, a backup job with the name "Server1" quickly identifies just those backup image files that are related to Server1.

The ShadowControl CMD console also uses backup job names in reporting on EndPoint status. Again, this makes managing these files easier.

Backup Comment

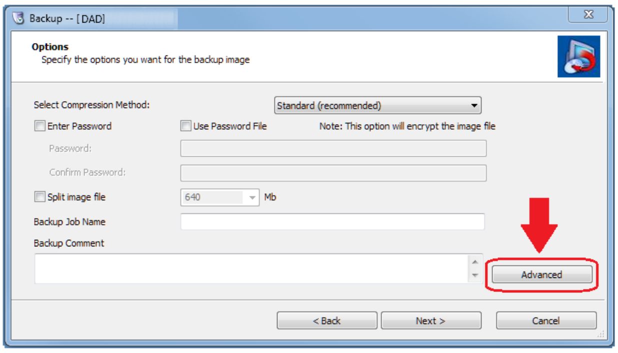
The Backup Comment option adds a text comment to a backup image file. Users can review these comments when mounting or restoring the backup image file at a later date. ShadowProtect adds the time and date stamp by default to the backup image.

ShadowProtect supports a text comment of up to 100 characters. The software displays an error message when attempting to save a comment exceeding this length. Return to the edit field to reduce the text length in order to save the comment.

Note: ShadowProtect includes the contents of this Backup Comment field in its log. Ensure that the text is clear and self-explanatory to avoid errors when reviewing the log files.

Advanced Options

ShadowProtect supports various advanced options for backup image jobs. Access these options by clicking **Advanced** on the Options page of the Backup Wizard:

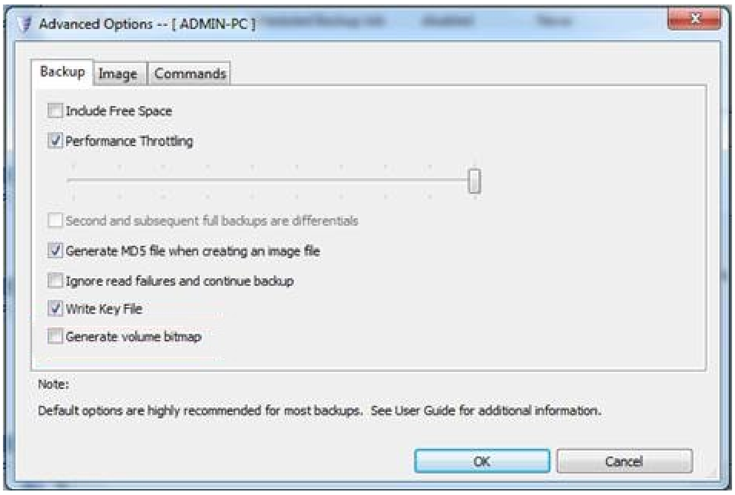

Backup -- [DAD]

Options
Specify the options you want for the backup image

Select Compression Method: Standard (recommended)
□ Enter Password □ Use Password File Note: This option will encrypt the image file
Password:
Confirm Password:
□ Split image file 640 Mb
Backup Job Name
Backup Comment

(For details on creating a job, see Creating Backup Image Files.)

⚠ **Note:** StorageCraft recommends keeping the default advanced option settings unless you fully understand the impact of changing these settings.


Advanced Options -- [ADMIN-PC]

□ Include Free Space
☑ Performance Throttling
□ Second and subsequent full backups are differentials
☑ Generate MD5 file when creating an image file
□ Ignore read failures and continue backup
☑ Write Key File
□ Generate volume bitmap

Note:
Default options are highly recommended for most backups. See User Guide for additional information.

ShadowProtect organizes these advanced options into four tabs:

- Backup
- Image
- Commands
- Retention

Note: Retention only appears when creating weekly or monthly backup jobs.

Backup

The Backup tab includes the following advanced options:

Option	Default	Description
Include Free Space	OFF	Backs up all sectors on the volume including those sectors marked as free space. This can result in a much larger image file, but can help preserve previously deleted files. **Note:** You can turn this option On or Off at a later date without creating a new job.
Performance throttling	ON, 100% I/O usage	Specifies how much I/O bandwidth that ShadowProtect can use when creating a backup image file. Use the slider bar to adjust this setting. Reducing (throttling) ShadowProtect I/O usage increases the time it takes to create a backup image file, but can reserve I/O bandwidth for other processes.

2nd and subsequent full backups are differentials	OFF	scheduled backup jobs. For example, if you have a weekly backup schedule that creates a new full image each Monday, selecting this option instructs ShadowProtect to create a differential image each Monday based on the changes since the initial full image. This reduces storage needs for the backup image files over time.
Generate MD5 file when creating an image file	ON	Instructs ShadowProtect to create an MD5 (Message Digest 5) checksum file when creating a backup image file. The checksum lets you confirm the file integrity of backup image files. ImageManager also uses this MD5 file to verify integrity.
Ignore read failures and continue backup	OFF	Instructs ShadowProtect to ignore disk read errors that occur during the creation of backup image files. Use this option with caution, as it may back up disk corruption and prevent a restored volume from working properly. However, in the event of a failed disk, it may help preserve any remaining intact data.
Write Key File	ON	Instructs ShadowProtect to create an SPK key file when choosing to encrypt backup files. Turning this option OFF forces ShadowProtect to not create an SPK file while encrypting backup files. Users will need to enter the encrypted file password each time to perform operations such as in ImageManager.
Generate volume bitmap	OFF	Causes ShadowProtect to create a bitmap file for the source volume. ImageManager can then use this file to prune free space during a backup consolidation. ShadowProtect's Image Conversion utility can also use this file to exclude free space when converting a file to VMDK or VHD.

Image

The Image tab includes the following advanced options:

Option	Default	Description
Enable write caching	OFF	Enables or disables using file caching when writing the backup image file. When writing to a network location, this may slow down the backup process.
Enable concurrent task execution	OFF	Enables or disables creating backup images simultaneously for multiple volumes rather than creating one backup image at a time. When using this option, the system hardware should support a high disk load.
Enable self-healing incremental recovery	ON	Determines how ShadowProtect reacts to a system error that interrupts the ShadowProtect incremental tracking feature. When set to Off, ShadowProtect recovers by generating a new full image and starting a new image set. When set to On, ShadowProtect recovers by creating an incremental image as planned, along with a differential image based on the most recent incremental image and the current volume. This prevents disruption of the incremental backup schedule. It can, however, result in increased CPU and network bandwidth usage when compared to creating a new set.
Auto-execution of unexecuted task	ON	Enables or disables executing the last scheduled backup job if it was missed. (For example, because the system was powered off.) If ShadowProtect missed more than one scheduled job, this option executes only the last unexecuted backup job.

Commands

The Commands tab specifies command files (.exe, .cmd, .bat) to execute at key points in the backup image file creation process. The command files cannot rely on any user interaction, so test each command file before using them with ShadowProtect. ShadowProtect allows 5 minutes at each stage (Pre-snapshot, Post-snapshot, and Post-backup) for command files to complete. If the command files do not complete in 5 minutes, ShadowProtect proceeds while the command files continue executing.

To use a command file for a particular stage, either:

- Use **Browse** to locate and open an existing command file or
- Enter the full file name, including path, into the appropriate field

Pre-Snapshot

Executes the specified command file before taking the image snapshot. For example, you might execute a pre-snapshot command file that places non-VSS-aware applications or databases into a backup state.

⚠ **Note**: It takes only a few seconds to create a snapshot, so non-VSS-aware databases or applications are only out of production briefly before they return to normal operating mode using a post-snapshot command.

Post-Snapshot

Executes the specified command file after taking the image snapshot. For example, you might execute a post-snapshot command file to return non-VSS-aware applications or databases back to normal operating mode.

Post-Backup

Executes the specified command file after creating the backup image file. For example, you might execute a post-backup command file to automatically copy the backup image file to an off-site location or FTP server.

⚠ **Note**: To avoid the 5 minute execution limit for post-backup command files, call a command file that executes another command file and then finishes. This lets you complete the ShadowProtect-associated command file in the 5-minute allotment while the secondary command file performs tasks that take longer to complete (synchronizing or copying the backup image files to an alternate location, scanning the backup image file for viruses, etc.).

Encryption

The Encryption tab specifies the algorithm used to encrypt the backup image file. This tab displays only when you select **Enter Password** on the Options page of the Backup Wizard (see File Protection).

Algorithm	Description
RC4 128-bit	Fastest, but least secure, algorithm
AES 128-bit	A balance between speed and security
AES 256-bit	The most secure, but slowest, of the algorithms

Note: Most contemporary hardware supports the default AES 256-bit encryption without undue delays.

Retention

The Retention tab sets policy for automatically managing the retention of backup images. ShadowProtect only displays the Retention tab for weekly or monthly jobs. (Continuous incremental jobs use ImageManager to enforce retention policy.)

The Retention tab includes the following options:

Option	Default	Description

Enable a retention policy	OFF	Enables or disables an automatic retention policy. The following settings outline this policy.
Number of backup Image Sets to retain	3	Specifies the maximum number of image sets to keep. When ShadowProtect reaches this set maximum, it deletes the oldest image set after running the next backup.
Delete both Full and Incremental backup images in the set	OFF	Instructs ShadowProtect to delete all files, both full and incremental, when removing an old image set. **Note:** By default, ShadowProtect enforces the retention policy (and deletes an older set) only after creating a new image set. This means that ShadowProtect creates the Maximum +1 image set first before deleting the oldest image set. This ensures that it always keeps the maximum number of image sets. However the drive storing the sets must have space for M+1 sets temporarily while ShadowProtect creates the newest backup.
Delete only Incremental backup images (retain Full backup images)	ON	Instructs ShadowProtect to delete only the incremental backup images when removing an old image set.
Enforce policy before starting the next Full backup	OFF	Instructs ShadowProtect to make room for a new image set by deleting the oldest image set *before* creating the new image set. This reduces the amount of disk space needed to adhere to the specified retention policy. **Note:** Use this setting to further limit the amount of space taken with backup files.

5.6 Deleting Backup Image Files

You can delete backup image files using any process you normally use to delete a file in Windows. However, before deleting a backup image file, be certain of the following:

- Verify that a full backup image file is not required for any existing chain from an active backup job. If this file is the start of an active backup job, deleting the file breaks the chain. If you proceed to delete the file, ShadowProtect will create a new full backup image file at the next scheduled backup and start a new chain. All existing incremental files in the old chain will not be accessible.
- Verfiy that no newer incremental files depend on an older incremental file before deleting the older one. If you proceed to delete the older file, all the later dependent backup image files become useless. That is, you cannot mount or restore files from these dependent backup image files.

Use the Image Conversion Tool to check for any incremental file dependencies.

6 Mounting Backup Image Files

The ShadowProtect Explore Backup Wizard guides you through the process of mounting a backup image file. If the selected image file is part of a chain, ShadowProtect automatically associates the files required to browse and restore this specific backup image file. You only need to select the backup image you want to explore. Once mounted, you can treat the backup image file as you would any other Windows volume:

- Browse the backup image file.
- Share the backup image file.
- Copy individual files and folders from the backup image file.
- Modify the backup image file (if the volume is configured as writeable).
- Use standard Windows security and file properties.

The restore process is the same whether you use the ShadowProtect console and Windows to restore files and folders or use the StorageCraft Recovery Environment to do so. Which you use depends specifically on the state of your system and what you need to restore:

Restore in Windows	Windows runs but you have lost data or had undesirable changes to applications or hardware files on a volume (excluding the operating system files).
Restore in Recovery Environment	Windows does not load and you have lost data or operating system files, or had undesirable changes to applications or hardware files on a volume. For more information, see the *StorageCraft Recovery Environment User Guide*.

⚠ **Note**: To restore data from an incremental image, you must have all previous incremental backup image files and the initial full backup image that the selected image depends on. If any of these files is missing or corrupt, mounting the backup image to that point in time is not possible.

For information about mount options, see Backup Image Mount Options.

ShadowProtect and Windows Deduplication Volumes

Microsoft supports its Deduplication (Dedupe) feature in Windows Server 2012 and newer operating systems. ShadowProtect supports Windows Dedupe in these situations:

- Mounting a backup image of a Windows dedupe-enabled volume if the mount occurs on a system with the Windows Dedupe feature enabled and the image file is stored on a non-dedupe-enabled volume.
- Restoring a backup of a Windows Dedupe volume. (Requires restoring to a system with the Dedupe feature enabled to access all files in the new volume.)

ShadowProtect cannot mount any backup file that is stored on a dedupe-enabled volume or dependent on another backup file that is stored on a deduped-enabled volume.

To mount a backup image file

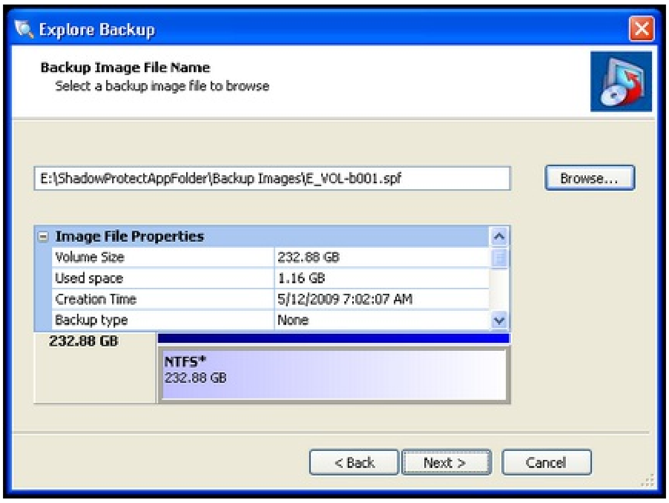
⚠ **Note**: To mount a VHDX backup on a system with a custom install of ShadowProtect, confirm that the system includes at least the ShadowProtect Backup Agent.

1. Use the Explore Backup Wizard in ShadowProtect to display the Backup Image File Name page.
2. Browse to the backup image file you want to mount, then click **Next**.
   For information about backup image file naming conventions, see File Naming Conventions.

   For NETGEAR ReadyDATA systems, enter the device's IP address or device name, then click **Browse**. In the Open dialog, Use the *Files of Type* dropdown box to change the default file type from *ShadowProtect files* to *VHDx*. Browse through the Completed Backups folder to select the desired point-in-time file to mount. The Mount Wizard selects the largest volume of a multi-volume VHDX by default. Select the desired volume to continue.

   ⚠ **Note**: You must provide the password for an encrypted backup image.

   The Explore Backup Image Wizard displays a categorized list of information about the backup image file.



Backup Image File Name

Select a backup image file to browse

E:\ShadowProtectAppFolder\Backup Images\E_VOL-b001.spf

Image File Properties	
Volume Size	232.88 GB
Used space	1.16 GB
Creation Time	5/12/2009 7:02:07 AM
Backup type	None

232.88 GB

NTFS*
232.88 GB

3. (Conditional) In the Backup Image Dependencies page, select the desired point-in-time image from the selected backup image set, then click **Next**.
4. On the Explore Options page, select how you want to mount the backup image, then click **Next**.
   For more information about mount options, see Backup Image Mount Options.

Mount Option	Procedure
Mount image as a drive letter	1. Select *Assign the following drive letter.* 2. Select the appropriate drive letter from the drop-down list.
Mount the backup image file as a mount point	1. Select *Mount in the following empty NTFS folder.* 2. Browse to an appropriate folder to select it. 3. To name the mount point subfolder, select to use: ▪ Time/Date (defaults to the image file's creation timestamp) ▪ File Name (defaults to the image file's name) ▪ Custom (a user-defined string)

5. (Optional) Deselect **Mount Backup as Read-Only** to mount the backup image as a writeable volume.
   If you mount the backup image file as a writeable volume, you can choose to save the changes to an Incremental image file when you dismount the volume (see Dismounting Backup Image Files in Windows).
   Note: Mounting a backup image as a writeable volume does not alter the source file. ShadowProtect never modifies an existing backup file.
   ⚠ **Warning:** NETGEAR ReadyDATA-stored VHDx backup image files may be mounted Writeable. However, that system does not support saving changes from a VHDx and discards them on dismount..
6. On the Wizard Summary page, review the mount information, then click **Finish**.
   ShadowProtect mounts the backup image file, automatically launches Windows Explorer and then displays the mounted volume.
7. With the backup image mounted, you can browse the contents of the volume as you would any Windows volume.
8. To restore individual files or folders, use Windows Explorer to copy them from the backup image file volume to your production volume.

   ⚠ **Note**: Once mounted, select Refresh Volumes Info to get an accurate view of the mounted system volumes from the Disk Map tab.

6.1 Recover Files and Folders

Use Windows Explorer to view and recover files and folders from backup image files. ShadowProtect adds two options to the Explorer's context menu (the right-click menu) of image files:

Mount	Launches the Image File Mount Wizard. This wizard guides you through the process of mounting the selected backup image file. This type of mount allows you to modify files or folders from the image file and then have ShadowProtect save those changes in a new backup image file. You can simultaneously mount multiple backup image files, but you must mount each backup image file individually with the Image File Mount Wizard.

Quick Mount	Mounts the selected backup image file as read-only using the next available drive letter. You can select multiple backup image files in Explorer then select Quick Mount to mount them simultaneously. Each mounted image file receives the next available drive letter. You can then copy files or folders from this mounted image to recover them.

Drives remain mounted until you dismount them or restart the machine. For more details about dismounting a backup image file, see Dismounting Backup Image Files.

NOTE: ShadowProtect retains NTFS file permissions in backup images. As a result, files or folders from a backup image may not open when using Quick Mount to view an image on a different system (which lacks those permissions). To temporarily change these permissions and view the files or folders, use Mount to open the backup image as Read/Write instead. Then use Windows Explorer to change ownership of the file or folder to access it.

6.2 Backup Image Mount Options

Decide which options to use for mounting a backup image file as:

- A drive letter
- A mount point
- Read-only
- Writeable

Drive Letter

The Mount Utility mounts a backup image file as a drive letter with all the properties of the original volume. For example, if an NTFS volume used EFS (Encrypted File System), this security remains intact on the volume when it is mounted.

You can perform a variety of tasks on mounted images: run ScanDisk or CHKDSK, perform a virus check, defragment the drive, copy folders or files to an alternate location or view disk information such as used and free space.

Once mounted, you can also set the image file as a shared drive. Network users can connect to the shared drive and restore their own files and folders.

Mount Point

You can mount an image file as a mount point (a directory on an NTFS file system). Mount points overcome the available drive letter limitation and support more logical organization of files and folders. The same functions that exist for drive letter mounts exist for mount points.

Read-Only

The ShadowProtect Quick Mount feature mounts image files as read-only. This provides access to the backup image to:

- Recover files
- View and verify the contents of the image
- Run other applications that need to access to the data from the backup image, such as a storage resource manager or data mining application

⚠ **Note**: Windows 2000 does not support mounting read-only NTFS volumes.

Writeable

ShadowProtect can also mount a backup image as a writeable volume. Users can then access the backup image to:

- Remove files from the backup image (such as running an anti-virus application to remove viruses, malware, etc.).
- Add files to create a new backup image.
- Update the backup image security.
- Change file and folder permissions
- Restore a backup image to a smaller volume (see Dismounting Backup Image Files).

⚠ **Note**: ShadowProtect tracks all these changes to the data and can then preserves these in a new image file when you dismount the image. This creates a new branch in the chain and is not used to continue the existing chain. The original image file is never changed.

Warning: ShadowProtect accepts the Writeable option for mounting VHDX-format backup image files stored on a NETGEAR ReadyDATA system. However, ShadowProtect discards all changes made to a ReadyDATA-sourced VHDX backup image file upon dismount.

Image Files and NTFS Permissions

ShadowProtect retains existing NTFS file and folder permissions for the volume. As a result, Windows prevents access to protected files or folders on mounted images without the correct credentials. To access protected files or folders, open the image as Read/Write using the Mount wizard. Use WIndows Explorer to then change ownership of the file or folder. (See Permissions for addtional details.)

Note: Using this Read/Write setting does work for VHDx files on a NETGEAR ReadyData system to change permissions on files and folders.

6.3 Dismounting Backup Image Files

Once mounted, a backup image file remains mounted until you dismounted it or the system reboots.

To dismount a mounted image:

1. Open the Backup Image Dismount Wizard by doing one of the following:
   - In the Tasks menu, click **Dismount Backup Image**.
   - In the Menu bar, select **Tasks** > **Dismount Backup Image**.
   - Right-click on the mounted image in Windows Explorer and click **Dismount**.
2. Use the Dismount wizard to:
   - Save changes (if mounted as writeable).
     ⚠ **Warning:** NETGEAR ReadyDATA-stored VHDx backup image files may be mounted Writeable. However, that system does not support saving changes and discards them on dismount..
   - Shrink the volume so you can restore the image to a smaller drive.

   ⚠ **Note**:The Shrink Volume feature truncates mounted backup image files so that the file system ends at the last currently-allocated cluster. To reduce the backup image size as much as possible, use a disk defragmentation tool on the mounted image to consolidate file distribution within the volume and free up space at the end of the volume.
3. In the Mounted Backup Images page, select the backup image volume to dismount. The wizard displays the volume properties.
4. Click **Next**
5. (Conditional) In the Backup Image Dismount Options page, select if you want to:
   - Save volume changes
   - Shrink the backup Image

   These options are available only if the backup image volume is writeable (see Backup Image Mount Options).
   Save changes to incremental File: Saves any changes made to the mounted volume. Right-click the incremental file to save the modified backup image file using a different name.

   ⚠ **Note**: In ShadowProtect 5.x and newer, we recommend modifying the backup image file name to clearly reflect its source. For example, if the source image file was C_VOL_b001-i119.spi then rename the modified backup image file C_VOL_b001-i119-i001.spi. (The i001 indicates it is the first incremental taken from the source image file i119.) However, with the release of ShadowProtect 5.2.0, the system automatically labels SPI files using a suffix similar to the above recommendation. For example, an SPI file generated from the image file C_VOL_b001-i119 now receives the label C_VOL_b001-i119-i001.spi.
   ShadowProtect does not create an MD5 file for SPI files. ImageManager will instead verify the integrity of SPI files using CRC rather than the MD5 file.

   Shrink Volume: Shrinks the volume so you can restore the image to a smaller hard drive partition. This option is only available when::

   - Dismounting a writeable backup image of an NTFS volume in Windows Vista, Windows Server 2008, jor newer versions of the OS.
   - Running the Mount feature in StorageCraft Recovery Environment.

     ⚠ **Note**: ImageManager may report an error when verifying an image file created from a mounted backup and which is shrunk from its original size.
6. Click **Next**.
7. In the Backup Image Dismount Summary page, review the dismount details, then click **Finish**.

   ⚠ **Note**: Once dismounted, select Refresh Volumes Info to get an accurate view of the mounted system volumes from the Disk Map tab.

Dismounting Images in Windows

Use Windows Explorer to dismount an image file. ShadowProtect adds two options to the Explorer's context menu (the right-click menu) for mounted image files:

Dismount	Launches the Backup Image Dismount Wizard. This wizard guides you through the process of dismounting the selected backup image file. Use this option for images mounted as writeable in order to save these changes to a new incremental file.
Quick Dismount	Dismounts the backup image file without any further user interaction. ShadowProtect dismounts the file without saving any changes to data.

7 Restoring a Volume

ShadowProtect provides two ways to restore a backup image file depending on which type of volume it is:

Volume Type	Restore using which ShadowProtect version	Description
Data Volume	ShadowProtect in Windows	Use the Restore Wizard in ShadowProtect to recover a data (non-boot) volume. **Note:** This method does not require you to reboot the system.
System (boot) Volume	Restore in the ShadowProtect Recovery Environment	Use the Recovery Environment to restore a system volume. **Note:** Use the Recovery Environment for Windows to restore from a VHD/VHDX formatted image file. The Recovery Environment CrossPlatform only supports restores from .SPF and .SPI image files, not from VHD or VHDX format files.

⛔ Warning: Restoring a backup image to an existing volume overwrites all data currently on that volume.

Supported Sector Sizes

Contemporary hard drives and SSDs ship with a 4096-byte *physical* sector size. Most also support the 512-byte *logical* sector size. (These drives are often labeled 512e for "512 Byte Sector Size Emulation".) ShadowProtect supports backing up both 4096- and 512-byte logical sector sizes.

In the unusual situation of restoring a partition/volume from one logical sector size to another:

- 512 bytes per logical sector -> 4096 bytes per logical sector (and the destination does not support 512e)
- 4096 bytes per logical sector -> 512 bytes per logical sector

ShadowProtect will issue an error message during the restore if it encounters a mis-matched sector size.

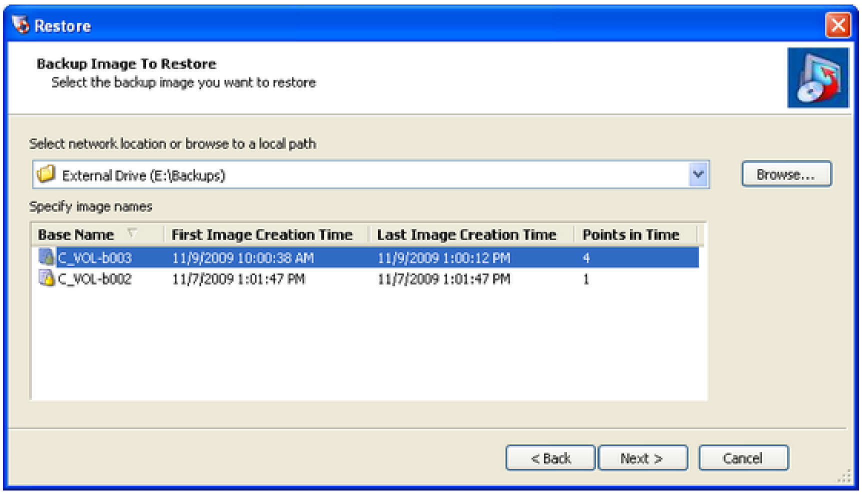
Restoring and Windows Deduplication

ShadowProtect can restore a backup from:

- an image file which contains a Windows Deduplication (dedup) volume. To access all the files in this vollume, the destination system needs to have the dedup feature eabled.
- an image file hosted on a dedup-enabled volume.

To restore a data volume

1. Open the Restore Wizard by doing one of the following:
   - In the Wizards tab, click **Restore**.
   - In the Tasks menu, click **Restore**.
   - In the Menu bar, select **Tasks** > **Restore**.
2. On the Backup Image to Restore page, select the Image Set to restore, then click **Next**.
   In the drop-down menu, select the destination (see Destinations) that contains the backup image set, or click **Browse** to locate the desired backup image set. The *Specify Image Names* field displays the backup image sets available at the selected destination or path.



Backup Image To Restore
Select the backup image you want to restore

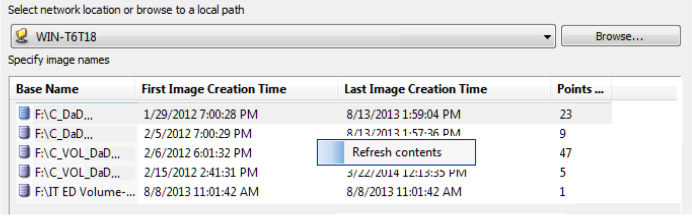
Select network location or browse to a local path: External Drive (E:\Backups)

Specify image names

Base Name	First Image Creation Time	Last Image Creation Time	Points in Time
C_VOL-b003	11/9/2009 10:00:38 AM	11/9/2009 1:00:12 PM	4
C_VOL-b002	11/7/2009 1:01:47 PM	11/7/2009 1:01:47 PM	1

⚠ Note: You must have the proper network credentials to access an image set stored on a network share.

3. If the *Specify Image Names* field does not list all the expected points-in-time, right-click on the list to display the option to refresh contents:

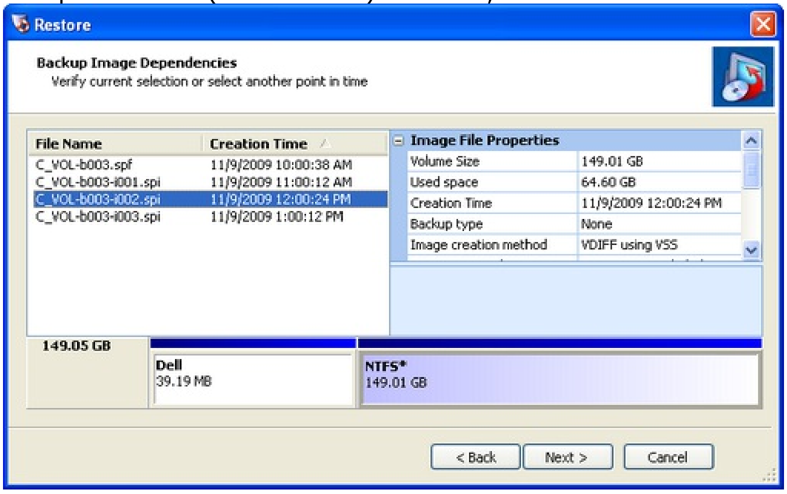


Select network location or browse to a local path: WIN-T6T18

Specify image names

Base Name	First Image Creation Time	Last Image Creation Time	Points ...
F:\C_DaD...	1/29/2012 7:00:28 PM	8/13/2013 1:59:04 PM	23
F:\C_DaD...	2/5/2012 7:00:29 PM	8/13/2013 1:57:36 PM	9
F:\C_VOL_DaD...	2/6/2012 6:01:32 PM		47
F:\C_VOL_DaD...	2/15/2012 2:41:31 PM	3/22/2014 12:13:35 PM	5
F:\IT ED Volume-...	8/8/2013 11:01:42 AM	8/8/2013 11:01:42 AM	1

4. Click **Refresh contents** to update the list of restore points.
5. Select which image set contains the point-in-time you wish to restore, then click **Next**.
6. On the *Backup Image Dependencies* page, ShadowProtect provides a list of times and dates of all the backups it has taken of the selected disk. Choose which point-in-time (date and time) to restore, then click **Next**.



Backup Image Dependencies
Verify current selection or select another point in time

File Name	Creation Time
C_VOL-b003.spf	11/9/2009 10:00:38 AM
C_VOL-b003-i001.spi	11/9/2009 11:00:12 AM
C_VOL-b003-i002.spi	11/9/2009 12:00:24 PM
C_VOL-b003-i003.spi	11/9/2009 1:00:12 PM

Image File Properties	
Volume Size	149.01 GB
Used space	64.60 GB
Creation Time	11/9/2009 12:00:24 PM
Backup type	None
Image creation method	VDIFF using VSS

149.05 GB — Dell 39.19 MB — NTFS* 149.01 GB

Note: This page also displays specific properties of the selected backup image file. These are informational only and are relevant when resolving restore issues with StorageCraft Support. These properties include:

Image File Properties	Shows the volume size and used space, creation time, backup type (none, daily, weekly, monthly), compression type, password protected (yes/no), and any comments.

Original Partition Information Style (MBR, GPT), number, type (FAT, NTFS), bootable option, offsets and length.

Disk Information Disk geometry, disk size, number of the first track sectors and if it is a dynamic disk. You can also view the disk layout graphically at the bottom of the screen. **Note:** This represents what the disk looked like at the time of backup.

Originating machine OS version, the machine name, MAC address, the ShadowProtect engine version used to create the image file and drive letter of the mounted volume.

7. On the *Restore Destination* page, select the partition where you want to restore the backup image, then click **Next**.

   ⚠ **Note**: The selected partition must have sufficient space for the selected restore. For example, you cannot restore a 40GB backup file to a disk or partition with only 10GB of free space. Uae the Disk Map tab to create or modify partitions as needed before doing the restore.

8. The Wizard displays the *Specify the Restoration Options* page. These options only apply to restoring System (boot) volumes (which is done using the Recovery Environment).. Click **Next**.
9. On the *Wizard Summary* page, review the details of the volume restore operation, then click **Finish**.

You can view the progress of the restore volume operation in the Backup Jobs tab.

⚠ **Note**: StorageCraft strongly recommends creating a new backup job for the restored volume. While an existing ShadowProtect backup job may continue to create new incrementals, issues arise from changes in hardware, volume size, or operating system between the pre-restore and post-restore incrementals. To ensure reliable backups, create a new job on the restored volume.

8 Image Conversion Tool

ShadowProtect includes the Image Conversion Tool to manage existing backup image files. This tool can:

- Convert a backup image into a virtual machine format (VMDK or VHD/VHDX).
- Consolidate a point-in-time backup image (full + incremental images) into a single new full image.
- Change the compression setting on an existing image.
- Change the encryption setting on an existing image.
- Split an backup image file into a Spanned Set where each file has a maximum file size. This is useful for moving backup image files to CD or DVD.

⚠ **Note**: Current hypervisors, including Hyper-V and VMware, will only mount a VMDK or VHD converted from partitions of less than 2TB. A workaround is to create multiple partitions smaller than 2TB on drives larger than 2TB. (See 2TB Limit using the Image Conversion Tool for details.) However, converting image files to VHDX does support greater than 2TB volumes.

Also, the conversion tool only supports FAT32 volumes up to 4GB in size--the limit for FAT32.

You can access the Image Conversion Tool from either Windows or the StorageCraft Recovery Environment.

Note: To exclude free space from the source file, set the **Advanced Options** > **Generate Volume Bitmap** option to ON when configuring the original backup job.

To use the Image Conversion Tool

1. In the ShadowProtect Tools menu at the left (or in the Tasks dropdown menu), click **Image Conversion Tool**.
2. The Image Conversion Tool wizard appears. Click **Next**.
3. On the Source Image File page, browse to the location of the backup image files you want to modify. ShadowProtect displays the a list of the backup chains stored in this location.

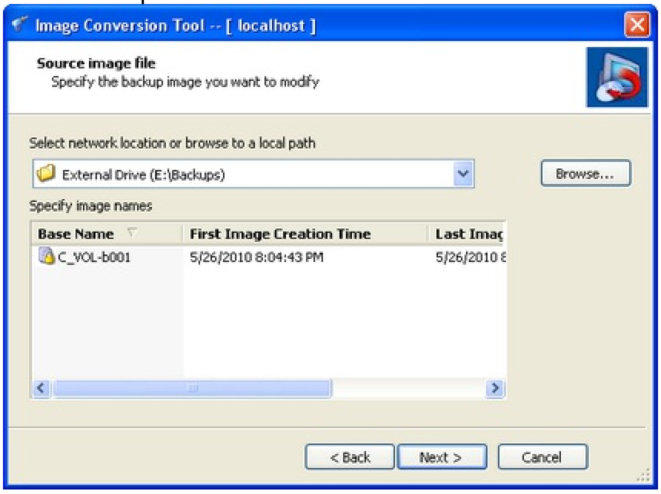


Image Conversion Tool -- [localhost]

Source image file
Specify the backup image you want to modify

Select network location or browse to a local path

External Drive (E:\Backups)

Specify image names

Base Name	First Image Creation Time	Last Imag
C_VOL-b001	5/26/2010 8:04:43 PM	5/26/2010 8

4. Select the chain by selecting the chain's full image file.
5. Click **Next**.

   ⚠ **Note**: Provide the password If the backup image is encrypted.

6. In the Backup Image Dependencies page, select the incremental image that represents the point in time you want. (The default is the full image.)

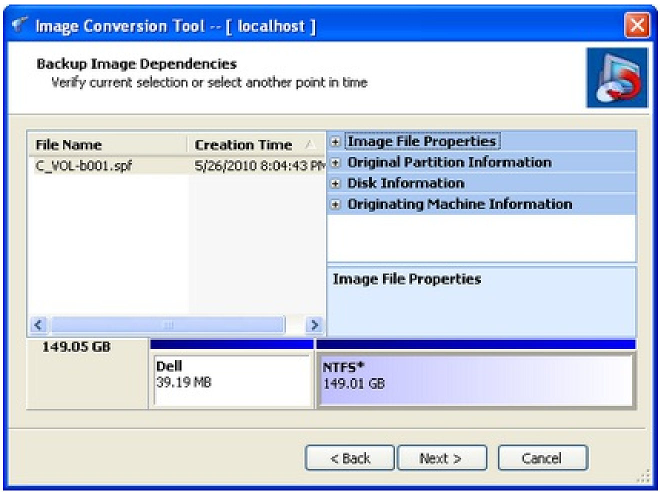


Image Conversion Tool -- [localhost]

Backup Image Dependencies
Verify current selection or select another point in time

File Name	Creation Time
C_VOL-b001.spf	5/26/2010 8:04:43 PM

ShadowProtect also displays the selected file's properties in four groups in the right panel:

- **Originating machine:** The operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.
- **Disk Information:** Disk geometry, disk size and number of the first track sectors. You can view the original disk layout in graphical form at the bottom of the screen.
- **Original Partition Information:** Style, number, type, bootable option, starting offset and length.
- **Image File Properties:** Volume size, creation time, compression, password protection, comment.

7. In the Destination Image File page, specify the required information, then click **Next**.

Select network location or browse to a local path	From the drop-down menu, select the Destination where you want to store the destination image file. If the menu doesn't show the path, click **Browse** to find the desired location.
Specify image name	Specify a name for the destination image file.

Save As	Select the type of image file you want to create. Supported options include: **SPF:** Creates a new full (base) image file by consolidating the original full image plus all the incremental files up to the point in time of the incremental selected. This full image can then be archived. **VHD:** Creates a Microsoft Virtual Hard Disk file compatible with Hyper-V virtual environments. **VHDX:** Creates a newer generation of Microsoft Virtual Hard Disk which supports volumes greater than 2TB. **VMDK:** Creates a Virtual Machine Disk file compatible with VMWare virtual environments. **NOTE:** Both the Recovery Environment-CrossPlatform and the one for Windows also support conversion of image files to .VHDx format.

8. In the Wizard Summary page, review the job summary, then click **Finish**.

   ⚠ **Note:** After converting a system volume backup image to a VHD or VMDK, make sure to load Recovery Environment in the VM first and run Hardware Independent Restore (HIR) using this converted system volume. Since the VM uses different hardware than the original system, you must do this before the operating system will boot successfully. If you still have boot problems refer to "Using HIR" and "Using the Boot Configuration Utility" in the *StorageCraft Recovery Environment User Guide*.
   Caution: Hyper-V currently does not support attaching and booting a VHDX file created from a system volume backup image.

The Image Conversion tool then creates the appropriate converted file.

Canceling an Image Conversion

Click **Cancel** to abort the conversion. For VMDK conversions, note that ShadowProtect creates a temporary file during the conversion. Unlike other StorageCraft products, the Image Conversion tool creates this temporary file with the actual name and .VMDK extension of the final completed conversion. After canceling this type of conversion, this temporary *.vmdk file may remain. This stub is incomplete and cannot be used for mounting.

8.1 2TB Limit using the Image Conversion Tool

The current hypervisor from VMware *only* supports VMDK files converted from partitions of under 2TB in size. Previous versions of Hyper-V also limited VHD files to under 2TB as well. Any ShadowProtect image file converted using the image conversion tool to VHD or VMDK format must come from a source partition that is under 2TB in total size. The actual size of the image file, even if it is under 2TB in size, isn't important. If the source partition is over 2TB then these hypervisors won't mount the file.

A workaround is to partition drives larger than 2TB into volumes smaller than 2TB.

NOTE: In Windows 8/Server 2012, Microsoft introduced a new virtual file format: VHDx. VHDx does support volumes greater than 2TB. ShadowProtect 5.2 and the image conversion tool do support this format. However, Hyper-V does not support attaching and booting a VHDX created from a system volume image file.

ShadowProtect warns if the source partition is larger than 2TB, depending on which version of ShadowProtect runs:

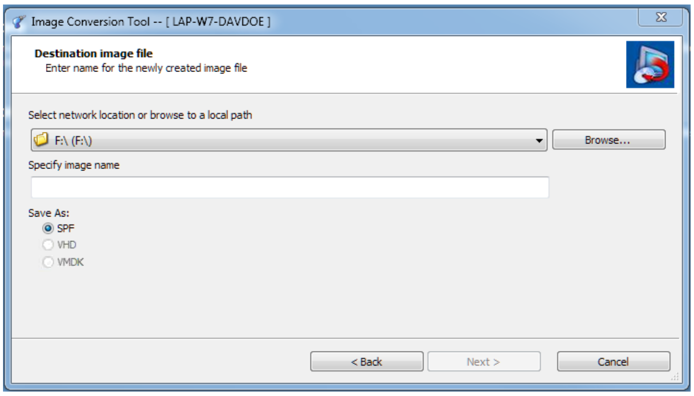
Warning in ShadowProtect versions 4.1.5 and older

When using the image conversion tool, ShadowProtect 4.1.5 and older will fail to create the converted file. Instead, it displays a -87 error in the event log:

```
14-Oct-2012 10:01:44 sbrest 411 Cannot create new virtual disk file E:\backups\big conversion.vmdk (-87 The
parameter is incorrect.)
```

ShadowProtect version 4.2.x and newer

In ShadowProtect 4.2 and newer, selecting a source partition larger than 2TB in the image conversion tool displays a dialog with the VHD and VMDK options disabled:



Destination image file

Enter name for the newly created image file

Select network location or browse to a local path

F:\ (F:\)

Specify image name

Save As:

● SPF

○ VHD

○ VMDK

9 Using ISOTool

ShadowProtect 5 includes an updated ISOTool. The new version can:

- Burn an ISO image to a disc (including CD, DVD, and Blu-ray),
- Mount and dismount ISO images
- Author a CD ISO. The authoring function can also modify an existing ISO image and save those changes to a new ISO file.

To use the ISOTool:

Note: Windows 2000 does not support ISOTool.

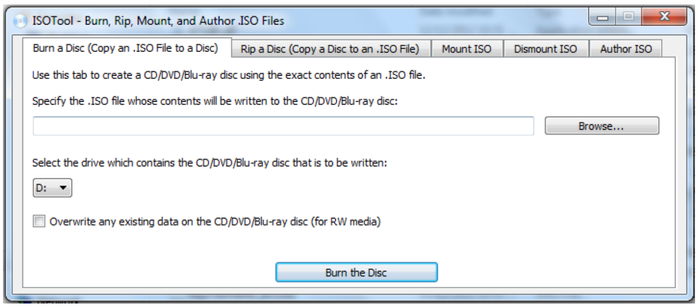
Run ISOTool either from:

```
Start/All Programs/StorageCraft/ISOTool.exe
```

or from

```
C:\Program Files (x86)\StorageCraft\ShadowProtect\ISOTool.exe.
```

Note: Either way, right-click on ISOTool.exe and select *Run as Administrator*.


ISOTool - Burn, Rip, Mount, and Author .ISO Files
Burn a Disc (Copy an .ISO File to a Disc)
Rip a Disc (Copy a Disc to an .ISO File)
Mount ISO
Dismount ISO
Author ISO
Browse...
Burn the Disc

Use this tab to create a CD/DVD/Blu-ray disc using the exact contents of an .ISO file.

Specify the .ISO file whose contents will be written to the CD/DVD/Blu-ray disc:

Select the drive which contains the CD/DVD/Blu-ray disc that is to be written:

D:

□ Overwrite any existing data on the CD/DVD/Blu-ray disc (for RW media)

The tool offers five tabs to:

- **Burn a Disc**
- **Rip a Disc**
- **Mount ISO**
- **Dismount ISO**
- **Author ISO**

These tabs provide instruction to perform these functions. The authoring tab has additional steps.

Author an ISO

Note: This option only creates non-bootable data disks.

To author a new ISO:

1. Double-click on the default name "My ISO" to enter another name.

2. Use the Disc Type dropdown box at the lower-right to specify what size image you want. The range is from 700MB to 128GB on a dual-layer Blu-ray disc.
3. Click **Add Files** to browse and select one or more files.
4. Click **Add Directory** to select a folder to include on the ISO.
   Note: ISOTool only accepts one folder at a time, even though you can select multiple folders at once.
5. To remove an unwanted folder or file, highlight one and click **Remove**.
6. Type in a name for the ISO.
7. Click **Browse** to select a destination for the new ISO.
8. Optional: check *Use Burner* to send the resulting ISO to a blank disc in the recorder.
9. Click **Author ISO**.

The ISOTool creates the new ISO image.

10 Using ImageReady

ShadowProtect 5 includes a new tool--ImageReady--for automated testing of backup image files. Specify a folder to manage and ImageReady automatically:

- Mounts each image in a backup job's set
- Runs a script against the mounted image
- Reports the results
- Saves any changes made to the mounted volume as an incremental for later testing

The results can verify the reliability for restoring fully-functional system, application, and data volumes.

For example, ImageReady can:

- Mount a volume and run Chkdsk to determine if there are problems with the data.
- Mount a Microsoft Exchange Server backup--including the system, data, and log volumes--and run a script that calls, for example, a test of the edb files to determine if they are intact or to run a cleanup process if the edb files are in a dirty shutdown state.

ImageReady Requirements

To run ImageReady:

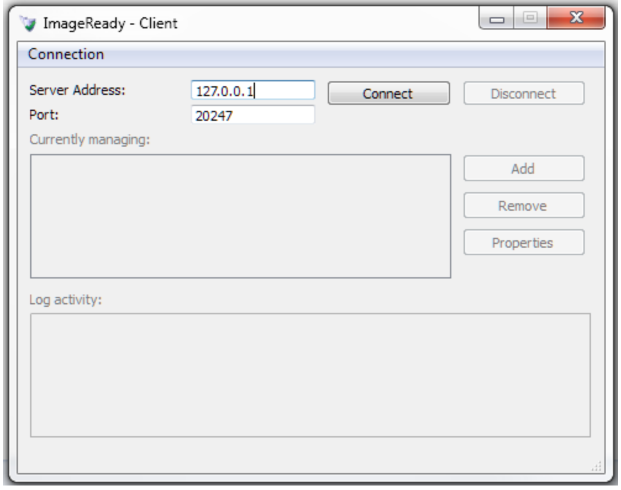
- The system firewall must have Port 20247 open for ImageReady to communicate.
- By default, ImageReady runs using the LocalSystem account on the workstation. For ImageReady to test image files stored on a network server or share, it needs rights to that folder or share. Either run the ImageReady service as Admin or grant the LocalSystem account credentials to log into the network resource.

Note: The Adobe CreativeCloud Suite install fails if the StorageCraft ImageReady service is installed and running. (The installer displays an error mesage that "The ImageReady service is already running.") On systems requiring CreativeCloud, use Windows Services.msc to stop and disable the StorageCraft ImageReady service prior to running the install. The StorageCraft ImageReady executables can also be deleted at that point if desired.

Note: Windows 2000 does not support ImageReady.

To use ImageReady:

1. Run ImageReady from the ShadowProtect folder. The ImageReady main dialog displays:



ImageReady - Client

Connection

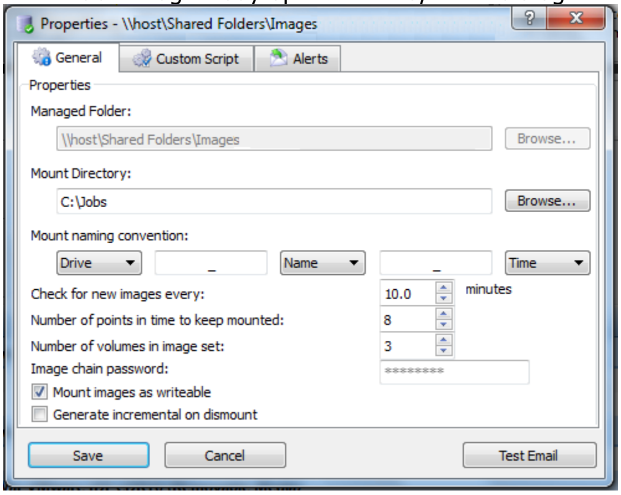
Server Address: 127.0.0.1

Port: 20247

Currently managing:

Log activity:

2. Click **Connect** to connect to the server.
3. Click **Add**. ImageReady opens the *Properties* dialog:



Properties - \\host\Shared Folders\Images

Properties

Managed Folder: \\host\Shared Folders\Images

Mount Directory: C:\Jobs

Mount naming convention: Drive _ Name _ Time

Check for new images every: 10.0 minutes

Number of points in time to keep mounted: 8

Number of volumes in image set: 3

Image chain password: ********

☑ Mount images as writeable

□ Generate incremental on dismount

4. On the General dialog, click **Browse** to select a folder that has or will have one or more backup image files.
5. Click **Browse.**
6. **S**elect a directory to use for mounting images.
7. Enter a unique name for the mounted image(s).
   ImageReady defaults to using:
   - the drive letter of the source image file
   - the source file's filename
   - the time of the mount

   to create a unique name for each mounted volume. ImageReady seperates these elements in the name with dashes but you can delete the dashes and customize the name as needed.

8. Select how often ImageReady checks the folder for new files to test.
   The range is from every 6 seconds to every 1440 minutes (ie: 24 hours or once a day) in 1/2 minute intervals.
9. Select the number of simultaneous mounted volumes ImageReady maintains--up to 96.
   This number of simultaneously mounted volumes is hardware- and hypervisor-dependent. ImageReady refers to these mounted volumes as "points in time" rather than "volumes" to reflect that a single server, such as Exchange, may require two or three volumes mounted simultanously in order to peform the required tests.
   Note: These settings cannot be changed once saved. Recreate the job if necessary to alter these settings.
10. If the selected image files are backups from a multi-volume set (such as with Microsoft Exchange), select the number of volumes to include.
11. Enter the password for encrypted backup image files in the *Image Chain Password* field.
12. Determine if the tests you want to perform need ImageReady to write to the mounted volumes. If so, check *Mount images as writeable*.
13. Determine if you want to preserve the results of any test which writes to a mounted volume. If so, check *Generate Incremental on dismount*.
14. Click **Save**.
15. Click *Custom Script* tab to enter the commands or script for ImageReady to run.
    This script can be of arbitrary length or as simple as c:\Windows\System32\chkdsk $MOUNTPATH1.

16. Specify a timeout in minutes or leave the default at 0 for unlimited.
    A timeout prevents a test from running an infinite loop.
17. Specify the number of concurrent tasks for ImageReady to execute.
    Note: ImageReady attempts to perform multiple mounts and tests concurrently. This number of simultaneously running tasks is hardware- and hypervisor-dependent. Should tests impact system performance, reduce the number of concurrent tasks.
18. By default, ImageReady only runs scripts on new image files in the managed folder. (That is, those files made after creating the ImageReady job.) Check *Apply to existing images* to have ImageReady run a script against all existing image files in the managed folder and not just new image files.
19. Check *Dismount on completion* to reduce ImageReady's demands on system resources.
    Otherwise, ImageReady will keep the volume mounted until:
    1) a new image file appears and
    2) it exceeds the number of points in time to keep mounted.
20. Select *Alerts* if you want the results of each test sent to an email address. Specify the details then click **Test Email** to confirm the configuration is correct.
    If you do not select to have the email alerts, information on the results will also appear in the Log Activity window of the main dialog.
    Note: Modifying alert settings for one job modifies the settings for all jobs.
21. Click **Save**.
22. Repeat these steps to add more folders or additional tests to run.

To edit an existing test, highlight the managed folder in the list and click **Properties**.

Error Messages

After clicking **Connect**, ImageReady may issue an error:

```
No connection could be made because the target machine actively refused it.
```

There are several possible causes for this error message:

Port Blocked: The most likely cause is that port 20247 is blocked at the firewall. Open this port to allow the ImageReady connection.

Lack of Connections: ImageReady uses connections to manage files and folders. When managing many folders or a folder with many image files, it may exhaust the available connections. At that point, ImageReady may issue the refused error.

This lack of connections may occur in Windows 7 or earlier desktop OSes, where Windows limits the number of connections available to applications. To manage many folders or many image files, use a Windows Server (including 2012) or a Windows 8 desktop to run ImageReady as these have no connection limitation.

11 Remote Management

ShadowProtect provides two ways to remotely manage ShadowProtect backup agents:

- Management View--Used for managing many nodes. Displays a list of nodes with their backup status. (ShadowControl CMD provides similar functionality.) Includes the option to do a push install of ShadowProtect on the node.
- Network View--Used for managing a smaller number of nodes on an individual basis.

Remote management requires access to these nodes over the LAN or through a virtual private network (VPN). By connecting to a remote node through one of these remote management tools, you have full access to the ShadowProtect features and functions on the remote node from this console.

⚠ **Note:** You must have administrative rights to the remote node in order to manage it. With administrative rights, you can remotely manage both ShadowProtect Server Edition and ShadowProtect Desktop Edition nodes using either the Management View or the Network View.

11.1 Management View

The Management View tab specifically manages ShadowProtect Server and ShadowProtect SBS installs with a large number of remote nodes from a central location.

Although its functionality is very similar to the Network View, the Management View simplifies administrator tasks when working with many remote nodes:

- Install the Backup Agent Remotely
- Add and Delete Remote Nodes
- Modify Remote Node Properties
- Connect and Disconnect Remote Nodes

Remote Install of Backup Agents

ShadowProtect can remotely install backup agents using the Push install wizard.

To remotely install a backup agent

1. In the Management View tab, click **Install**. ShadowProtect displays the Push Install Wizard.
2. On the *Specify Installer Package* page, click **Browse** to select the ShadowProtect Installer Package.
3. Click **Next**.
   Note: There must be an associated installation setup file (.iss) with the selected installer package. For more information, see Creating an Install Setup Package.
4. In the *Choose Search Options and Proper Credentials* dialog box, provide the required information, then click **Next**.

   System Name
   The name of the system where you want to install the ShadowProtect Backup agent. Select either **Domain name** or **Host name** according to the type of system name you are providing, then type the system name in the field.

   ⚠ Note: If you leave the field blank, Push Install uses your current domain or workgroup to locate a list of available systems.

   Use Active Directory Search
   Instructs ShadowProtect to search Microsoft Active Directory for the desired system.
   If you select to use AD, the wizard enables the **Options** menu at the bottom of the dialog box to refine the Active Directory search characteristics.

   Use Specified Credentials
   The authentication credentials that Push Install uses to gain access to the remote system.

   ⚠ **Note:** If you do not provide credentials, Push Install uses your current credentials to attempt to access the remote system.

   Discover Services
   Push Install attempts to identify existing ShadowProtect services running on a remote system. When successful, it displays the information it gathers about the agent version.

   Automatically activate installed agents
   Instructs Push Install to automatically activate the Backup agent after installation.
   To use this feature, click **Settings** (at the bottom of the Push Install dialog box when **Automatically activate installed agents** is selected) to specify the username and serial number of the ShadowProtect license you want to use on the remote system.

   Reboot after install
   Instructs ShadowProtect to automatically re-boot the remote system after installing the agent. (The agent requires a reboot.)
   To use this function, click **Settings** (at the bottom of the Push Install dialog box when **Reboot after install** is selected). Specify the details of the reboot operation. These details include setting a specific date or time for the reboot; specifying a message to display before rebooting; and specifying a delay before the reboot occurs (in seconds) after the message displays.
5. (Conditional) If you did not specify a system name to receive the agent earlier, you can use the *Computers Overview* page to select the systems you want. Click **Next**.
6. On the Install Overview page, wait until the install finishes. Click **Next**.
7. (Optional) On the Post Install Overview page, specify a Group name for each system where you installed backup agents. For more information about Groups, see Modifying Remote Node Properties.
8. On the Summary page, click **Finish**.
   The newly installed remote nodes appear in the Management View node list.

Adding and Deleting Remote Nodes

To manage a remote node, you must add it to your Management View.

To add a remote node

1. In the Management View tab, click **Add**.
2. In the Server Details dialog box, specify the appropriate connection information for the remote node.
   For information about remote node properties, see Modifying Remote Node Properties.

You can now connect to the remote node to manage ShadowProtect.

To delete a remote node

1. In the Management View tab, select the remote node in the node list.
2. Click **Delete**.
   Note: Deleting a remote node only removes it from the Management View. It does not delete ShadowProtect or any of its configurations from the remote node. Also, it does not remove the remote node from the Management View function of any other system that might be configured to remotely manage that node.

⚠ **Note:** You cannot delete the local node from the Management View.

Modifying Remote Node Properties

The properties table displays the properties of the currently selected remote node.

⚠ **Note:** You can edit the remote node's descriptive properties when it is connected. You can edit the login credentials only when it is disconnected.

To modify the properties of a remote node

1. Open the Network View in the console.
2. In the node list, select a remote node to modify.
3. If the console doesn't display the Properties pane, click **Properties**.
4. Modify the remote node properties as needed in the pane.
   Select a field to make it active. (You can also use the tab key to move from field to field.)

Remote node properties include:

Server Name Displays the machine name for the remote node used in the node list.

Server Address Shows the IP address or machine name of the remote node. Click **Browse** … to locate a particular system and identify its IP address.

Group Name The group that you want to associate with the remote node. Groups help organize remote nodes which share similar characteristics or requirements.

- Without a Group Name for the node, ShadowProtect lists the Node as an Unmonitored Node. The ShadowProtect management console will not try to actively connect to the node and monitor it.
- Once the node has a Group Name listed, the Node appears under the Group Name. The ShadowProtect Management console will try to automatically connect to the node each it launches to monitor the node.

Server Description Displays a user-deffined description of the remote node.

Status Indicates the remote node's status (connected or disconnected).

Domain Name Enter the domain name used to access the remote node.

User Name Enter a user name with administrator rights to the remote node.

Password Enter the user name's password.

Agent Version Displays the version of the ShadowProtect backup agent installed on the remote node.

Last Connected Displays the date and time this console last connected to the remote node.

Connecting and Disconnecting Remote Nodes

To connect to a remote node

1. In the Management View tab, select the remote node in the node list.

2. Click **Connect**.
   You connect to only one node at a time. If you try to connect to another node, ShadowProtect automatically disconnects you from the first one.

   ⚠ **Note:** You must add a remote node to the Management View in order to connect to it (see Adding and Deleting Remote Nodes).

To disconnect a remote node

1. In the Management View tab, select the remote node in the node list.
2. Click **Disconnect**.

   ⚠ **Note:** Disconnecting from a remote node does not stop the ShadowProtect backup agent or affect any of the ShadowProtect operations on that remote node.

11.2 Network View

The Network View displays a list of monitored nodes in a panel at the right side of the ShadowProtect console. Use **Network View** in the View menu to display it.

Network View can:

- Add and Delete Remote Nodes
- Modify Remote Node Properties
- Connect and Disconnect Remote Nodes
- Export and Import Node Settings

Adding and Deleting Remote Nodes

You must add each remote node to your Network View to manage it.

To add a remote node

1. If the console doesn't display the Network View, click **Network View** from the View menu.
2. In the Network View, click **Add**.
   This creates a new node named *New Node 1*. It also opens a Properties pane beneath it where you can configure the remote node.
3. In the Properties pane, enter the credentials needed to connect to the node.
   For information about remote node properties, see Modifying Remote Node Properties.

You can now connect to and manage the remote node.

To delete a remote node

1. In the Network View, select the remote node in the node list.
2. Click **Delete**.
   Deleting a remote node does not delete ShadowProtect or any of its configurations from the remote node. It also does not remove the remote node from the Network View of any other system that might be configured to remotely manage that node.

⚠ Note: You cannot delete the local node from the Network View.

Modifying Remote Node Properties

The Properties table displays details of the selected remote node.

Note: You can edit the remote node's descriptive properties when it is connected. You can edit the login credentials only when it is disconnected.

To modify properties of a remote node

1. If the Network View is not visible in the console, select **Network View** from the View menu.
2. In the node list, select a remote node to modify.
3. If the console doesn't display the Properties pane, click **Properties**.

4. In the Properties pane, modify the remote node properties as needed.
   Select a field to make it active. You can also use the Tab key to move from field to field.

Remote Node properties include the following:

Server Name Displays the machine name for the remote node.

Server Address Shows the IP address or machine name of the remote node. To browse the network for a particular system so you can find the IP address, click Browse ....

Group The group that you want to associate with the remote node. Groups help organize remote nodes which share similar characteristics or requirements.

- Without a Group Name for the node, ShadowProtect lists the Node as an Unmonitored Node. The ShadowProtect management console will not try to actively connect to the node and monitor it.
- Once the node has a Group Name listed, the Node appears under the Group Name. The ShadowProtect Management console will try to automatically connect to the node each it launches to monitor the node.

Server Description Displays a user-deffined description of the remote node.

Status Indicates the remote node's status (connected or disconnected).

Domain Name Enter the domain name used to access the remote node.

User Name Enter a user name with administrator rights to the remote node.

Password Enter the user name's password.

Agent Version Displays the version of the ShadowProtect backup agent installed on the remote node.

Last Connected Displays the date and time this console last connected to the remote node.

Connecting and Disconnecting Remote Nodes

To connect to a remote node

1. If the console doesn't display the Network View, select **Network View** from the View menu.
2. In Network View, select the remote node in the node list.
3. Click **Connect**.
   You connect to only one node at a time. If you try to connect to another node, ShadowProtect automatically disconnects you from the first one.

   ⚠ **Note:** You must add a remote node to the Network View in order to connect to it (see Adding and Deleting Remote Nodes).

To disconnect a remote node

1. In the Network View, select the remote node in the node list.
2. Click **Disconnect**.

   ⚠ **Note:** Disconnecting from a remote node does not stop the ShadowProtect backup agent or affect any of the ShadowProtect operations on that remote node.

Exporting and Importing Node Settings

ShadowProtect lets you transfer remote node configurations from one ShadowProtect console to another. This saves having to reenter these configurations at the new console.

To export remote node configurations

1. If the console doesn't display the Network View, select **Network View** from the View menu.
2. In the Network View, click **Export nodes**.
3. Specify a name for the XML file that contains the configurations, then click **Save**.

To import remote node configurations

1. In the Network View, click **Import nodes**.
2. Browse to the XML file that contains the exported configurations, then click **Open**.

11.3 Using an Install Setup Package

A ShadowProtect Install Setup Package contains the settings needed for an automated push installation of the software. ShadowProtect includes two setup package files: one for a full (which includes all utilities) and one for a backup-agent-only install.

You can find these setup files on the ShadowProtect CD or you can download them from the StorageCraft website.

⚠ **Note**: Each setup package is unique to the ShadowProtect version it installs. Confirm that the package file has the same name as the ShadowProtect Installer package but with a .iss extension.

To use the ShadowProtect Install Package

1. Save the appropriate .iss file (Agent or Full) and the ShadowProtect installer to the same folder on a local drive. ⚠ **Warning:** Avoid directory names with spaces for .iss installs. The install may fail if the command line program attempts to interpret paths with spaces in directory names.
2. Click **Install** in the Management View tab. The Push Install wizard opens.
3. Click **Next** to open the Specify package dialog.
4. Click **Browse** to locate and select the ShadowProtect installer. The wizard populates the details.
5. Use the wizard to enter credentials, locate the desired system, install and activate ShadowProtect on that system.

   ⚠ **Note**: You can select one or more systems within the selected domain. However, you can only activate one system, not multiple systems, using the push wizard. To activate multiple systems, use the Management View to select each unactivated system and apply a license to the system.

Silent and Remote Install EULA

Regardless of the installation method, by installing, retaining, copying, accessing, or using the software, you are accepting and agreeing to the terms of the End User License Agreement for Select StorageCraft Software Products ("EULA") which can be found here.

By installing the software, you either (i) accept and agree to the terms of the EULA as the end user, or (ii) if you are installing the software on behalf of an entity or other end user, you represent that the end user has accepted and agreed to the terms of the EULA and that you are authorized to accept the EULA on behalf of such end user.

12 Using VirtualBoot

VirtualBoot boots a system volume backup image into a Virtual Machine (VM) environment without performing a restore operation or converting backup files to a different format. By leveraging the open source Oracle VirtualBox software, VIrtualBoot provides a quick, temporary replacement system for a failed server.

VirtualBoot provides an innovative solution to the following situations:

System Fail-over: Restoring a failed system with terabytes of storage using traditional methods can take days. A VirtualBoot replacement can take minutes and gives users full access to system resources and applications after only a brief downtime to cut-over to the new system.

Backup Test: Few administrators perform backup and restore tests using traditional methods. VirtualBoot can mount any backup image in a VM for testing to make sure a restored system would function properly.

Access Application-specific Data: While backing up data is a critical operation, sometimes the data files alone aren't useful without their associated applications. VirtualBoot can mount an entire system, both applications and data, in a VM where you have access to data within its associated application.

For information about VirtualBoot usage scenarios, see VirtualBoot Scenarios.

This section includes the following topics:

- VirtualBoot Requirements
- Limitations
- Creating a VM
- Configuring a VM Manually

Note: DeveloperNotes_VirtualBoot.txt contains developer-level information related to VirtualBoot. You can find this file in the *<install_folder>*\StorageCraft\ShadowProtect\ folder. This file gives troubleshooting and advanced technical details for using VirtualBoot.

Warning: If you want to power off a VM created with VirtualBoot, do *not* select *Restore current snapshot VirtualBoot* as a shutdown option. You will lose all data written in the VM since its creation. Select this option *only* if you want to revert the VM back to its original state.

Also, do not launch a VM with VirtualBoot if the source system:

- is still active on the same network
- runs continuous incremental backups using ShadowProtect
- saves its backup files to a network share or NAS system.

Doing so will mix backups from the VM with those from the source system. Mixing backups corrupts the chain and prevents a valid restore of the volume.

12.1 VirtualBoot Requirements

VirtualBoot requirements include those of ShadowProtect and VirtualBox:

Software Requirements

Note: StorageCraft reommends upgrading to the latest build of VirtualBoot, v4.3.12, for maximum and reliable performance.

ShadowProtect 4.*x* or later: VirtualBoot supports backup image files created by any version of ShadowProtect, but you must have ShadowProtect 4.*x* or later installed to run the application. ShadowProtect 4.*x* includes VirtualBoot as a core component of the console installation.

Note: Although VirtualBoot can generate a VM from backup image files created with any version of ShadowProtect, StorageCraft recommends using VirtualBoot with backup image files created by ShadowProtect 3.3 and later to get full access to the benefits of VirtualBoot.

VirtualBox: VirtualBox is an open source VM environment from Oracle. VirtualBoot provides native support for ShadowProtect files in a VirtualBox VM. For information about VirtualBox and to download the software, visit www.virtualbox.org.

ShadowProtect supports various versions of VirtualBox up through v4.3.12. Please refer to the *VirtualBoot Developer Notes* found in the ShadowProtect directory for details on the latest supported versions.

Warning: VirtualBoot does not support VirtualBox 4.0.0 as that version does not properly use third-party plugins.

Hardware Requirements

VirtualBoot hardware requirements are driven primarily by the hardware requirements necessary to run VirtualBox (see VirtualBox End-User Documentation).

Processor: Oracle recommends using a recent (last five years) "reasonably powerful" x86 processor (either Intel or AMD), including AMD/Intel x64 processors. VirtualBoot does not support Itanium (IA64).

Note: When using VirtualBoot to boot an image of an x64 operating system, make sure that your host hardware supports AMD-V or VT-x, and that AMD-V, or VT-x, is enabled in the host machine's hardware BIOS settings.

Memory: At least 1GB

Hard Drive: At least 10 GB. This is dependent upon the guest operating system you want to load in the VM.

Host OS: VirtualBoot supports the same host operating systems as VirtualBox 1.6; namely Windows XP or later. Windows 2000 is not supported.

Guest OS: VirtualBoot supports backup image files that contain backups of the following operating systems (this is the OS that runs in the VM):

- Windows 2000
- Windows XP (32- and 64-bit)
- Windows 2003 (32- and 64-bit)
- Windows Vista (32- and 64-bit)
- Windows 2008 (32- and 64-bit)
- Windows 2008 R2 (32- and 64-bit)
- Windows 7 (32- and 64-bit)
- Windows 8 (32- and 64-bit)
- Windows Server 2012 and R2

12.2 Limitations

This release of VirtualBoot has the following limitations:

- Supports boot volumes only up to 2TB. However, VirtualBoot supports data volumes (non-bootable) of any size.
- Does not support UEFI-based system volumes.
- Does not support LBD/4K hard disk volumes which report 4096-byte sector size to the OS. However, Advanced Format hard disks, which have 4096-byte sectors but report 512-byte sectors to the OS, are supported.
- Performing a virtual boot of Windows Small Business Server (SBS) may require 16GB or more to deliver full functionality.
- If the host crashes while running a VirtualBoot VM, you must create a new VM using the latest Incremental backup image file created in the VM. (This requires having ShadowProtect run on the VM.) For more information, see the VirtualBoot Scenarios.
- VirtualBoot does not run in a Windows 2000 Terminal Services session.
- VirtualBoot does not support NETGEAR ReadyDATA VHDX backup files of system volumes.

Note: Windows Activation may intentionally lock some OEM copies of Windows to specific machines. This may also be true of various applications. Some OEM licenses may, in fact, not reactivate except on the original machine. In these cases, using VirtualBoot to launch a Windows VM based on a Windows OEM license or include applications with restricted licenses may run for only a limited period without activation. Consult with Microsoft or the application vendor on reactivation options.

12.3 Creating a VM

Important: Before using VirtualBoot to create a VM, review the VirtualBoot Requirements and Limitations.

To create a virtual machine

1. Start VirtualBoot using the.

   Executable: In Windows, select **Start** > **All Programs** > **StorageCraft** > **ShadowProtect** > VirtualBoot.exe.

   Command Line: From a Windows command prompt, move to the Program Files (x86)\StorageCraft directory. Type `VirtualBoot` *<backup image file>*, where *<backup image file>* is the name, including full path, of the ShadowProtect backup image file that you want to use to create a VM. For example:

   ```
   VirtualBoot e:\backups\C_VOL-b005.spi
   ```

   Right-Click Menu: In Windows Explorer, right-click the ShadowProtect backup image file that you want to use to create a VM, then select **VirtualBoot**.
2. Click **Next** on the VirtualBoot Wizard welcome page.
3. In the Backup Image List page, provide the required information, then click **Next**.

If you start VirtualBoot using the command line or right-click menu option, VirtualBoot populates the Backup Image list with all files that are part of the backup chain for the specified backup image file.

Add Image File	Adds a backup image file to the VM. Use this if you have a separate data volume you want to include in the VM. **Note:** VirtualBoot attempts to automatically include all volumes that are part of the boot volume's image set in this list. When this does not occur, use this option at add in these other volumes. If the selected backup image file is encrypted, you must provide a valid password to access it. **Caution:** Use care when selecting image files from multiple backup jobs. If the VM executes incremental backups, those created for volumes that are not in the boot volume's image set likely won't be useful or reliable.
Remove Image File	Removes a backup image file from the VM.
Specify Boot Volume	Designates the boot volume in the VM. Typically, VirtualBoot detects this automatically, but if you include multiple bootable volumes in the VM, you can specify which volume serves as the boot volume. To do so, select the volume you want from the list and click **Specify Boot Volume**.

⚠ **Note:** If you specified a backup image file when starting VirtualBoot, this page lists the related backup image file information.

4. In the Options page, provide the required information, then click **Next**.

Specify the operating system for the new virtual machine	From the dropdown menu, select the Windows OS installed on the boot volume of the backup image file.
Automatically create the new virtual machine	Instructs VirtualBoot to automatically create the VM as part of the configuration process. If you do not select this option, you must manually configure the VM in VirtualBox. In either case, VirtualBoot creates the XSP files that VirtualBox uses to define the virtual disk drives in the VM. ⚠ **Note:** VirtualBoot ALWAYS places the boot volume in the Disk_0 XSP file. For more information, see Mounting a VM Manually.
Automatically start the new virtual machine	Select this option to launch VirtualBox automatically after the VM is complete and load it for use.
Specify the name of the new virtual machine	Specify a name for the VM. By default, VirtualBoot creates a name based on the machine name.
Specify the amount of memory to allocate to the new virtual machine	Specify the amount of memory, in MB, that VirtualBox should allocate for use by the VM when it loads.
Specify the VM network adapter type	Select whether to include a network adapter in the VM. Supported options include: **NAT PRO/1000 MT Desktop:** Adds a generic network adapter to the VM that uses Network Address Translation (NAT). **No Network Adapter:** Excludes a network adapter from the VM.

5. (Optional) On the Options page, click **Advanced** to open the Advanced Options dialog box.
The Advanced Options dialog box provides the following options:

Import only one volume per hard disk drive within the virtual machine	Instructs VirtualBoot to include only one volume per VirtualBox XSP file. By default, VirtualBoot assigns four volumes per XSP file. ⚠ **Note:** VirtualBoot ALWAYS places the boot volume in the Disk_0 XSP file.
Deactivate Windows within the virtual machine	Deactivates Windows on the VM's system volume. Because Microsoft licensing limits the number of reactivations, this option lets you use the activation grace period to accomplish your purposes with the VM. ⚠ **Note:** If the host hardware where you start the VM is sufficiently different, Windows might deactivate automatically.
Store write buffers in a different directory than the image files	Lets you specify a location to store the write buffers used when creating the VM. By default, VirtualBoot stores write buffers in the same location as the backup image files used to create the VM.
Override personality used to configure the virtual machine OS volume	For use by StorageCraft technical support only.

6. On the Wizard Summary page, click **Finish**.

VirtualBoot generates the files necessary to support the new VM and, if specified in the VM configuration, creates the VM and launches it for use.

⚠ **Note:** For information see Mounting a VM Manually.

7. You may need to do further configuration on the VM if, for example, you want to use the VM as a temporary replacement for a server. If so, continue with Configuring a VM and refer to the VirtualBox documentation for details.

To Restart an existing Virtual Machine

You can also restart an existing VM manually from VirtualBox:

1. Launch VirtualBox.
2. In the left-side VM list, select the VM, then click **Start**.

Continuing Incremental Backups

You can continue a ShadowProtect backup job with the VirtualBoot temporary replacement of a failed server. Continuing the backup job is critical, as otherwise all updated content is lost when the VM shuts down. When working with a VirtualBoot VM backup job, consider these best practices:

- To prevent performance problems in the VM, use only Incremental backups (see Creating Backup Image Files). Do not use differential imaging.
- ShadowProtect places a backup job for the source volume used in the VirtualBoot VM in a Paused/Disabled state. After starting the VM replacement, manually re-start the backup job (found in the Backup Jobs tab) to continue making incremental backups from the replacement volume on the VM.
- If you power down a VM created with VirtualBoot, do NOT select **Restore current snapshot VirtualBoot** as a shutdown option. This discards all changed data written in the VM since its creation. Select this option *only* if you do want to discard these changes and revert the VM back to its original state. (This might be useful when performing a backup or restore test.)

To continue incremental backups in the VM

1. Launch your VM using either VirtualBoot (by selecting the relevant image file in Windows Explorer) or VirtualBox (by selecting the appropriate pre-existing VM).
2. Once the VM loads, log in, then start ShadowProtect in the VM.
3. In ShadowProtect, select the Destinations tab.
4. In the Destinations tab, select the destination object used to store the VM's source backup image files, then click **Edit**.

   ⛔ **Warning:** Do not delete the destination object or you will break the backup image chain. Rather, modify the destination object as needed to point to the current location of the backup image files used to create the VM.

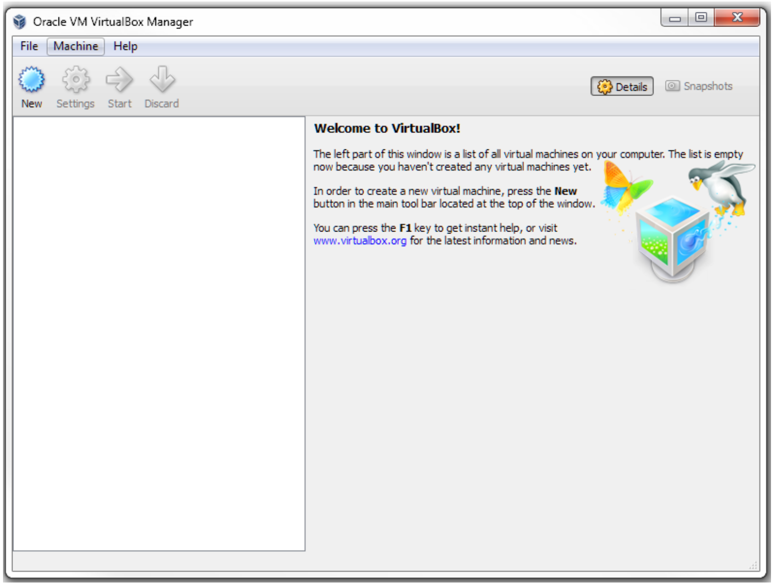
5. In the Destination dialog box, modify the Destination Path to point to the location of the backup image files used to create the VM. Click **OK** when done.
   You might need to modify the network credentials (Domain, User, Password) in the destination object to access the backup image files in their new location.
   - If you have problems with name resolution in the VM environment, try using the IP address of the host machine rather than its Host name.
   - When editing the Destination Object path, use only real SMB/CIFS network share paths. Do not use share paths provided in the VM-to-Host file sharing facility of the VirtualBox "Guest Additions".
6. In the ShadowProtect main page, select the Backups tab.
7. Select the appropriate backup job, then click **Execute**.
   ShadowProtect restarts the job with a new incremental backup in the existing chain. (The naming of incremental backup files in the VM starts where the last Incremental image file used to create the VirtualBoot VM left off.) This maintains a single backup image chain for the server and makes it possible to provide Head Start Restore (HSR) capabilities.

   ⛔ **Warning:** When you are ready to put the restored server back online and shut down the VM, you will want to remove the VM configuration from VirtualBox. Howvever, be sure the restoration is complete before removing the VM from VirtualBox. Any incremental backups created in the VM are dependent upon the initial VirtualBoot incremental backup image file. If you remove the VM, VirtualBox deletes this file. (You can identify this file because the file name includes a long numeric GUID value). If the initial image file is deleted, then all subsequent incrementals created in the VM unusable. (This is similar to deleting a chain's initial SPF image file, which would also render all subsequent incrementals unusable.)

Mounting a VM Manually

Once you use VirtualBoot to create the VM and later dismount it, you can use VirtualBox to manually mount the VM later on. StorageCraft strongly recommends using the automated VirtualBoot process instead.

⚠ **Note:** The following task is based on VirtualBox v 4.2.4. Task details might vary slightly with different versions of VirtualBox.



Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for the latest information and news.

To manually create a virtual machine

1. Launch VirtualBox.
2. If the VM exists in the list at the left, select it and click **Start**.
3. If the VM does not exist in the list, click **New** from the menu bar. VirtualBox launches the *Create Virtual Machine* wizard.
4. Enter a name for the VM.
5. Select the Guest OS and version.
6. Click **Next**.
7. Specify the amount of RAM.
8. Select *Do not add a virtual hard drive* and accept the caution. VirtualBox creates the VM.
9. Select the VM from the list. Click **Storage** in the specifications section to the right. VirtualBox displays the Storage Settings dialog.
10. Click the *Add Hard Disk* icon.VirtualBox asks if you want to add a disk.
11. Click **Choose existing disk**.
12. Navigate to the .XSP file for use with this VM. Typically this is in the same folder with the volume's image files. (VirtualBoot virtual hard disk files have a .xsp extension.These XSP files contain lists of the backup image files that constitute the virtual hard drive used by the VM.)
13. Click **OK** to accept the disk configuration.
14. Select the new VM from the list.
15. Click **Snapshots** in the upper-right of the VirtualBox Manager.
16. Click the Take a Snapshot icon at the upper-left of the Current State dialog.
17. Enter a name and description for this snapshot. Click **OK**. VirtualBox takes a snapshot of this VM.
18. Right-click the VM in the list. Click **Start**. VirtualBox runs the VM.

Once created, you can start the VM manually from VirtualBox at any time by selecting it from the list and clicking **Start**.

Configuring a VM Manually

Once you configure a VM for use with VirtualBox, you can use the VM for testing as well as a replacement server. You can adjust various configurations for testing:

- Configuring Drivers
- Installing Guest Additions
- Configuring a Network Adapter
- Continuing Incremental Backups

⚠ **Note:** When working with a VM, you must be able to switch keyboard/mouse focus between the VM and your system environment. To switch focus to the VM, simply click the mouse in the VM window. To switch focus out of the VM, press the right Ctrl button.

Configuring a Network Adapter

You can choose to not have a network adapter in the VM if you want to boot a backup image while the source system is still operational. Keeping both systems operating with the same network configuration can cause the following:

- Routing problems particularly at the Domain controllers.
- Both the VM and the source system might save Incremental backup images to the same network location. While this does not affect data integrity, it can lead to confusing backup image file names with Incremental backup image files from both branches of the chain intermixed and erratic results with consolidation.

Keeping the VM off the network lets you resolve these types of issues before they cause any problems. For example, once the VM loads you can pause ShadowProtect backup operations in the VM.

To change network support to the VM

1. Launch VirtualBox.
2. On the VirtualBox main page, select the VM where you want to add a NIC, then click **Settings**.
   The VM must be powered off to modify the VM settings.
3. On the Settings page, select **Network** in the left-side navigation.
4. Select the Adapter 1 tab, then select to enable or disable the Network Adapter.
5. If you choose to keep the adapter enabled, then in the **Attached To** field, select how you want the virtual NIC to communicate with your host.
   By default, VirtualBox uses Network Address Translation (NAT), but it supports other connection options. For more information, see the VirtualBox documentation. A Bridged Adapter is necessary if you want VM services to be visible to other network hosts. For example, during a failover scenario for an Microsoft Exchange server.
6. Click **Advanced**, then select the virtual adapter type to use in the VM.
   In testing, the "Intel Pro/1000 MT Desktop" appears to be a good generic driver for the VirtualBoot environment.
7. Click **OK** to modify the network adapter settings.

Configuring Drivers

After starting a VM for the first time, Windows may detect a configuration change in the VM environment.

To configure drivers

1. Allow Windows to identify hardware and install drivers in the VM.
   Windows goes through its initial boot sequence, identifying hardware and attempting to load drivers for those devices. This process is similar to performing a Hardware Independent Restore (HIR) in ShadowProtect. Follow the on-screen prompts and allow Windows to reboot as needed to load the necessary drivers.
2. After rebooting, log in to the VM.

⚠ **Note**: Because of hardware changes detected by Windows as part of the transition to the VM environment, Windows will likely prompt you to reactivate Windows when you log in to the VM. However, you typically have a three-day grace period for doing this. Because Microsoft restricts the number of hardware reactivations for each Windows license, you might want to leave Windows deactivated if you can get the production system ready to restore within the three day grace period. If this is not possible, activate Windows in the VM using the standard Microsoft activation process, and your Windows VM is licensed for as long as you need it. If your Windows installation does not grant a login grace period and requires immediate reactivation, try booting into Safe Mode, or Safe Mode with Networking, to log in.

Installing Guest Additions

You can install VirtualBox additions to provide enhanced interaction with, and control over, the VM environment.

To install VirtualBox guest additions

1. From the menu bar in the VM, select **Devices** > **Install Guest Additions**.
   This loads a virtual CD into the VM that has extra software designed to make the VM run quickly and smoothly. If the CD does not auto-run, browse the CD drive in the VM and execute one of the following:
   - **`VBoxWindowsAdditions-x86.exe`**: `32-bit Windows VM.`
   - **`VBoxWindowsAdditions-amd64.exe`**: `64-bit Windows VM.`
2. Follow the directions in the Guest Additions Wizard, then reboot the VM.
3. Log in to the VM.

13 Other Operations

ShadowProtect includes additional features to maintain your backup environment:

- Verification of Backup Image Files
- Email Notifications
- Log Files
- Creating Key Files
- Recovery CD

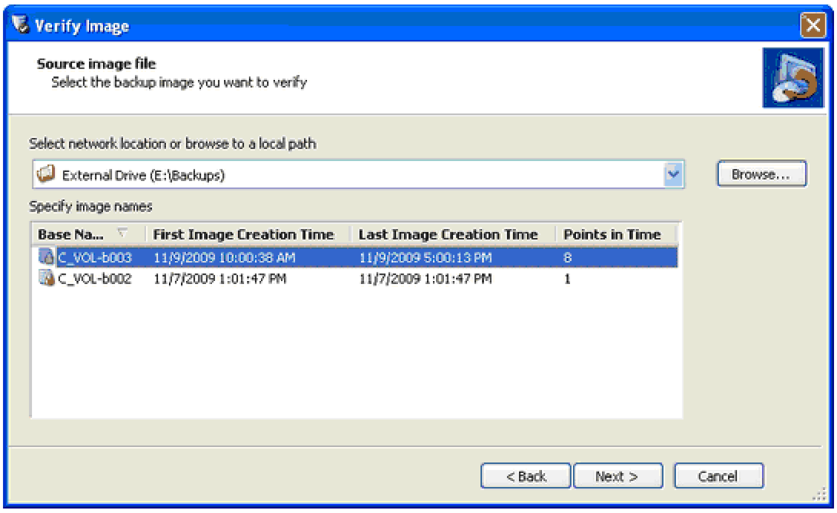
13.1 Verifying Backup Image Files

StorageCraft recommends performing verfication of backup images to ensure that each image is ready for recovery. ShadowProtect provides three ways to verify the quality of a backup file:

- Use Mount or Quick Mount to open a backup image. Browse the folders and open various files. If you can do this successfully, you know the backup image is healthy.
- Use ImageReady to automatically run tests on mounted volumes. (See Using ImageReady for details.)
- Use the Verify Image tool in ShadowProtect to test the integrity of a specific backup image.

To test a backup image with the Verify Image tool

1. Open the Verify Image Wizard in the ShadowProtect console:
    - In the Tools menu, click **Verify Image**.
    - In the Menu bar, select **Tasks** > **Verify Image**.
      ShadowProtect displays the Verify Image Wizard.
2. Click **Next**.
3. On the *Source Image File* page, select the image set to verify.



Verify Image

Source image file
Select the backup image you want to verify

Select network location or browse to a local path

External Drive (E:\Backups)

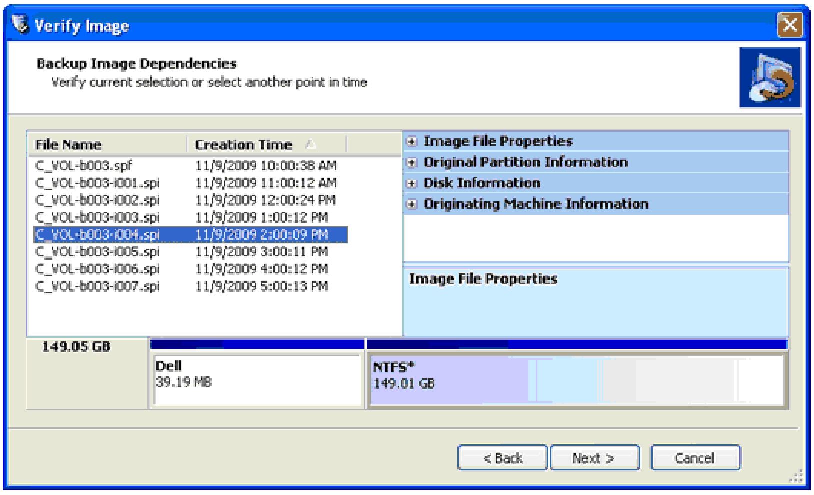
Specify image names

Base Na...	First Image Creation Time	Last Image Creation Time	Points in Time
C_VOL-b003	11/9/2009 10:00:38 AM	11/9/2009 5:00:13 PM	8
C_VOL-b002	11/7/2009 1:01:47 PM	11/7/2009 1:01:47 PM	1

⚠ **Note:** You must have the proper network credentials to verify a backup image set stored on a network share.

4. Click **Next**.

5. On the *Backup Image Dependencies* page, select the point in time to verify.



Verify Image

Backup Image Dependencies

Verify current selection or select another point in time

File Name	Creation Time
C_VOL-b003.spf	11/9/2009 10:00:38 AM
C_VOL-b003-i001.spi	11/9/2009 11:00:12 AM
C_VOL-b003-i002.spi	11/9/2009 12:00:24 PM
C_VOL-b003-i003.spi	11/9/2009 1:00:12 PM
C_VOL-b003-i004.spi	11/9/2009 2:00:09 PM
C_VOL-b003-i005.spi	11/9/2009 3:00:11 PM
C_VOL-b003-i006.spi	11/9/2009 4:00:12 PM
C_VOL-b003-i007.spi	11/9/2009 5:00:13 PM

This page displays all Incremental backup image files associated with the selected image set. Select a specific backup image file to view its properties:

Image File Properties: Shows the volume size and used space, creation time, backup type (none, daily, weekly, monthly), compression type, password protected (yes/no), and any comments.

Original Partition Information: Style (MBR, GPT), number, type (FAT, NTFS), bootable option, offsets and length

Disk Information: Disk geometry, disk size, number of the first track sectors and if it is a dynamic disk. You can also view the disk layout graphically at the bottom of the screen. **Note:** This represents what the disk looked like at the time of backup.

Originating machine: OS version, the machine name, MAC address, the ShadowProtect engine version used to create the image file and drive letter of the mounted volume.

5. Once you select the point in time you want to verify, click **Next.**
6. On the *Specify the Verify Options* page, select what you want to verify**:**

Verify only selected image: The Verify Image tool checks only the selected backup image file.

Verify selected image and all dependent files: Verifies the selected backup image file and all files that it depends on. This process verifies the integrity of the full point-in-time backup. If you select this option, specify the order to verify the files (Newest to Oldest or Oldest to Newest).

7. Click **Next**.

8. On the *Wizard Summary* page, review the details of the verify operation, then click **Finish**.

You can view the progress of verify operations in the Backup Jobs tab of the console.

13.2 Configuring Email Notifications

ShadowProtect can send email notifications on the success or failure of a backup job with details on its start and finish time, source volume, and destination.

To configure email notifications

⚠ **Note:** Verify your external email account has POP/IMAP support enabled

1. In the menu bar of the console, select **Options** > **Agent Options**.
2. On the Agent Options page, provide the details of the email configuration:.

   SMTP Server Name or IP Address The host name or IP address of the outgoing SMTP server to use when sending email notifications (for example smtp@gmail.com).

SMTP Port	(Default: 25) The port used by the SMTP service. The default port for secure SMTP connections (SSL) is 465.
SMTP Login User Name	The username ShadowProtect uses to access the SMTP server. For example, jdoe@email.com.
SMTP Login Password	The password associated with the SMTP user name.
SMTP Authentication Method	The authentication method used by the SMTP server. Select the appropriate authentication method for your SMTP server from the dropdown list. For example, the SMTP authentication method for Gmail is Login.
Use SSL	(Default: Off) The selection for a secure connection with the SMTP server. When using SSL, make sure to set the SMTP Port accordingly. (The SSL port is 465.)
Email From Address	The email address that appears in email message's From field.
Email To Addresses	A list of email addresses that you want to receive the notification. Use a semi-colon for multiple addresses.
Custom Subject Suffix	(Optional) A text string that appears below the ShadowProtect-generated email content in the Subject field. When creating this content, use /r for carriage return, /n for new line, and /t for tab characters.
Custom Body Prefix	(Optional) A text string that appears in the email Message field. Use /r for carriage return, /n for new line, and /t for tab characters.
Send Email on Success	(Default: Off) The selector for notifying success. Select ON if you want to send notification emails when ShadowProtect successfully completes a job.
Send Email on Failure	(Default: Off) The selector for notifying failure. Select ON if you want to send notification emails when ShadowProtect fails to complete a job.
Send daily report	(Default: Off) The selector for daily notifications. Select ON if you want to send a daily report of ShadowProtect activities.
Send weekly report	(Default: Off) The selector for weekly notifications. Select ON if you want to send a weekly report of ShadowProtect activities.

3. Click **OK** to save the configuration.
   Note: You need to select ON for at least one type of email (Success, Failure, Daily or Weekly) to receive email notifications.
4. (Optional) Click **Test Email** to send a test message and confirm that the email configuration is working properly.

If you have trouble receiving ShadowProtect email messages on your production email server, try sending emails to an external email account such as Gmail or Outlook. This lets you isolate the problem to ShadowProtect or the email system.

13.3 Log Files

ShadowProtect creates a log file for each backup job. This file shows the backup job results, including the reason for failure, if any. You can view the log for any backup job in the Backup History Tab.

The log shows:

- Start Time
- End Time
- Type (Full or Incremental)
- Source
- Destination
- Status

Backup jobs that finished successfully have a status of "Completed." Jobs that did not complete successfully have a Warning icon⚠ and a note such as "Execution Failed" or "Aborted." It is important to review these entries and determine why the job failed.

The second half of the job log provides information about the events that occurred during that job:

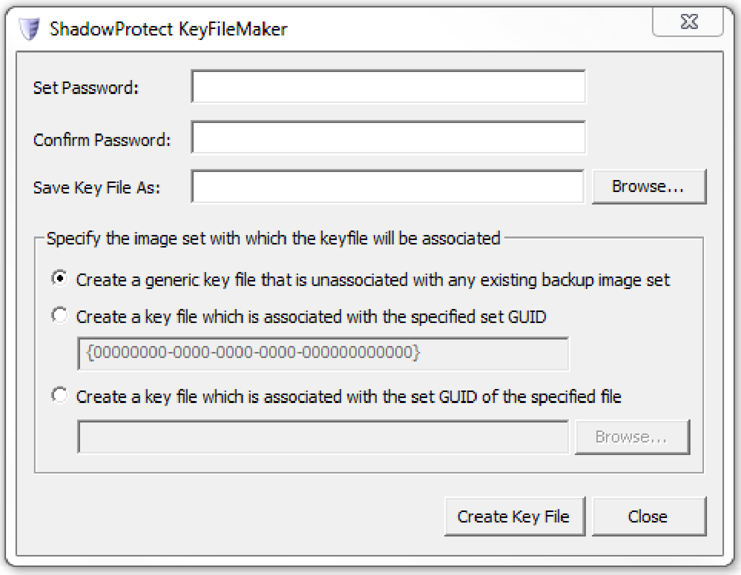
- Timing (when the event occurred)
- Module
- Code
- Message

ShadowProtect marks any event that did not complete successfully with a failed icon.☒. Use this information for troubleshooting and working with StorageCraft Support.

13.4 Creating Key Files

Key Files store passwords for encrypted backup images. Using key files lets you delegate the creation and storage of encrypted backup image files without losing control of the passwords. (For example, a user assigned to run ImageManager can configure it to do collapses of encrypted files without the user needing access to the passwords.) Key files have a `.spk` file extension with a prefix that matches the name of the associated full backup file. ShadowProtect includes the KeyFileMaker tool for recreating lost or corrupted Key Files.

⚠ **Note:** ShadowProtect automatically generates a new Key File each time it creates a new full backup with encryption activated.



ShadowProtect KeyFileMaker

Set Password:

Confirm Password:

Save Key File As:

Specify the image set with which the keyfile will be associated

● Create a generic key file that is unassociated with any existing backup image set

○ Create a key file which is associated with the specified set GUID

{00000000-0000-0000-0000-000000000000}

○ Create a key file which is associated with the set GUID of the specified file

To create a key file

1. Launch KeyFileMaker (**Start** > **Program Files (x86)** > **StorageCraft** > **KeyFileMaker** > **KeyFileMaker.exe**).
2. In the KeyFileMaker dialog box, provide the following information, then click **Create Key File**.

Set Password / Confirm Password	Specify the password to store in the Key File.
Save Key File As	Specify the name and location for the Key File. You must save the Key File in the same folder as the backup image files that rely on it.
Key File Association	Specify the backup Image Set that you want to associate with this Key File. **Generic Key File:** The key file is not associated with any backup image set. Select *Generic Key File* if all the backup image files in a given folder are part of the same image set. **Key File associated with a specific GUID:** Select this option if you have multiple backup image sets in the same directory and you want to manually specify the File Set GUID (Globally Unique ID) for the image set associated with this Key File. You can locate this GUID if you: a. Extracted the File Set GUID from one of the set's image file's header information. (All backup image files in an image set share the same File Set GUID.) b. Viewed the File Set GUID by starting to mount an image file from the relevant set with the Mount wizard (in Windows Explorer), then locating the GUID in the *File set GUID* field on the Image File Name page. **Key File associated with a specified backup image:** Use Browse to locate an image file in the set you want associated with this Key File. The tool automatically extracts the GUID for use in creating the Key File.

KeyFileMaker creates the new Key File in the specified folder.

13.5 Creating a Recovery CD

StorageCraft provides two types of Recovery Environment to restore a system volume:

- Recovery Environment for Windows--Created using the RE Builder tool. RE Windows (REWIND) is a 32-bit application.
- Recovery Environment CrossPlatform--Available as an ISO for download in either 32- or 64-bit versions.

Either tool can restore Windows system volumes. Both have a similar interface. The difference is that the REBuilder application creates REWind using a seperate downloaded WinPE while REX is a self-contained Linux-based environment.

Refer to the RE Builder documentation for details on creating a REWind disc.

To create a Recovery Environment CrossPlatform disc

1. If necessary, download the Recovery Environment Crossplatform ISO image file.
   1. Open a Web browser to the StorageCraft Recovery Environment ISO Download web page.
   2. In the Serial Number field, specify the product serial number you received when you purchased ShadowProtect.
   3. Click **Submit**.
   4. Accept the EULA.
   5. Select which version of the Recovery Environment to download: 32- or 64-bit.
   6. Save the ISO image to a local drive.
2. Insert a blank CD/DVD/Blu-Ray disc in your system's optical drive.
3. From Windows, select **Start** > **All Programs** > **StorageCraft** > **ISOTool**. The ISOTool runs.
4. On the Burn a Disc tab, click **Browse** to select the RE CrossPlatform ISO file.
5. Select the optical drive (the default is D:).
6. (Optional) Select **Overwrite any existing data...** if you want to replace existing data on the disc.
7. Click **Burn the Disk**.
8. When ISOTool finishes transferring the ISO image, click **Close**.
   Note: This ISO transfer can take several minutes to complete.
9. Test the Recovery disc by rebooting your system using the disc.

14 Best Practices

Turn off disk defrag software when using incremental backups. When ShadowProtect takes an incremental backup, it writes a file identifying those sectors that changed since the last backup. Disk defrag software change many sectors on the disk. This greatly increases the time it takes to run the next incremental backup. If you want to run disk defrag software, do it before running a full backup image. Then do not run or schedule the disk defrag software to run while ShadowProtect is scheduled to take Incremental backup images.

Test the StorageCraft Recovery Environment. Make sure the ShadowProtect Recovery Environment CD boots your system and that you have access to both any local drives and network devices that you might need.

Monitor disk space usage where ShadowProtect stores backup images. If the location runs out of space, backup jobs fail.

Monitor the ShadowProtect log file. Routinely examine the ShadowProtect log file. The log file confirms the success or failure of a job. Should a backup job fail, the log file provides details allowing you to take corrective action.

Use password encryption to protect backup image files. ShadowProtect backup images include all the contents of the disk drive. Using password encryption protects this data.

Include multiple volumes in your backup job. Databases or applications may span or use multiple volumes. Be sure to include all relevant volumes--not just the data volume--in the backup image. ShadowProtect snapshots can operate simultaneously on multiple volumes, ensuring cross-volume consistency.

Periodically save backup image files to removable storage. External hard drives or optical media let you store backup image files at an off-site location to keep images available in the event of an onsite disaster.

Use the Image Conversion Tool to manage backup images. You can consolidate backup images, split backup images for CD or DVD storage, or save the images as virtual disks. You can also use ImageManager for consolidating continuous incremental backup jobs.

Use Email notification. Automatic emails keep you informed of the operation of your ShadowProtect backup jobs. You can then quickly identify and resolve problems.

Use a retention policy that maximizes point-in-time histories. Review the Retention option available in ShadowProtect for retaining point-in-time histories, including using differential images for second and subsequent full images. These options can maximize the use of available storage capacity.

Working with heavily stressed servers. When monitoring the operating conditions of critical servers, you may note that one or more systems (such as Windows SBS) become heavily-tasked during business hours. This burden may result in failed VSS backups. Rather than opting for only a crash-consistent backup using a non-VSS driver, ShadowProtect often can successfully execute a VSS backup of these same server volumes by scheduling the VSS backup outside of normal business hours when the server is less tasked. (See Creating Backup Files for details on scheduling.)

Reinstall after an OS upgrade. An OS upgrade drastically changes the system. Whether it is an upgrade from an existing Windows 7 system to Windows 8 or a Windows 8 to a Windows 8 Pro, these changes impact ShadowProtect. To ensure consistent ShadowProtect performance, deactivate the ShadowProtect license and uninstall the software prior to the upgrade. After the OS upgrade, reinstall ShadowProtect and reactivate the license. Even if the system preserves the old backup job configurations and other ShadowProtect settings, StorageCraft recommends starting a new backup job for the upgraded system rather than continue an existing chain based on the earlier OS version.

Snapshot driver fails to install. The ShadowProtect snapshot driver, stcvsm.sys, may not install as a result of a conflict with the Windows Telnet Service. This can lead to failed backups and errors in the Windows Event logs. For this failure to occur, the Windows Telnet Service must be:

- Installed
- Running
- The "Log On on type" changed to "Local System account"
- The "Allow service to interact with desktop" option unchecked.

This failure may also issue various error messages:

In the ShadowProtect Backup log

- Cannot lock the volume (-5 Access is denied.)
- Unexpected end of the image file
- Final error (-5 Access is denied.)
- sbrun.exe started successfully but failed to complete the task
- Incrementals are not supported on this volume

In Windows Application Event log (all VSS errors)

- VssAdmin: Unable to create shadow copy: The shadow copy provider had an error.
- Volume Shadow Copy Service error: Unexpected error DeviceIOControl
- Volume Shadow Copy Service error: Unexpected error calling routine CoCreateInstance.
- Volume Shadow Copy Service error: A critical component required by the Volume Shadow Copy service is not registered.

To avoid this install failure and other errors, keep the Telnet default setting of:"Local Service". (For further details, see the Microsoft KB article.)